info@wazuh.com
https://wazuh.com

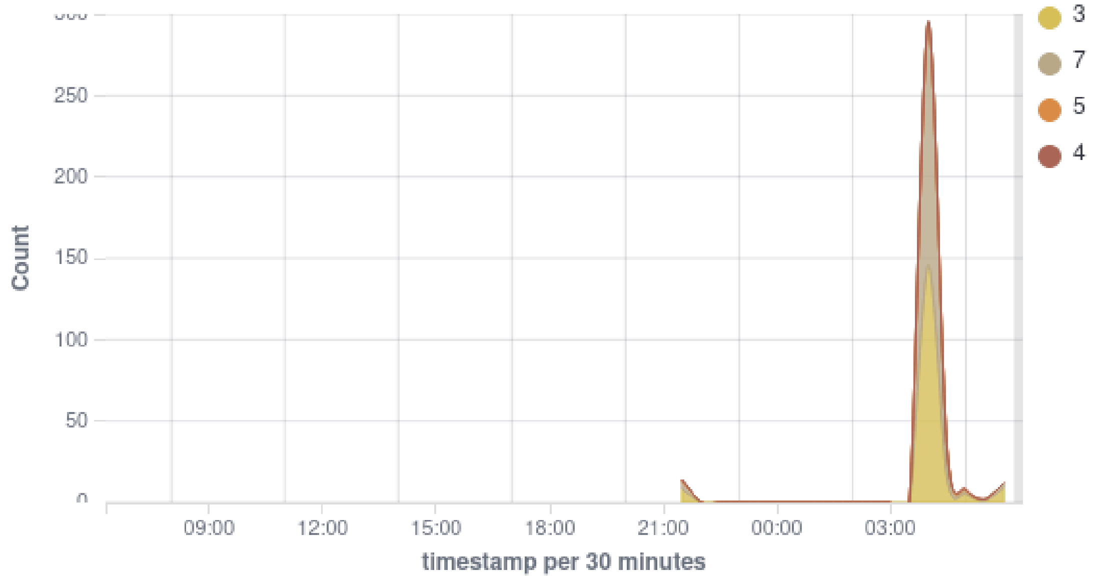
Threat hunting report

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

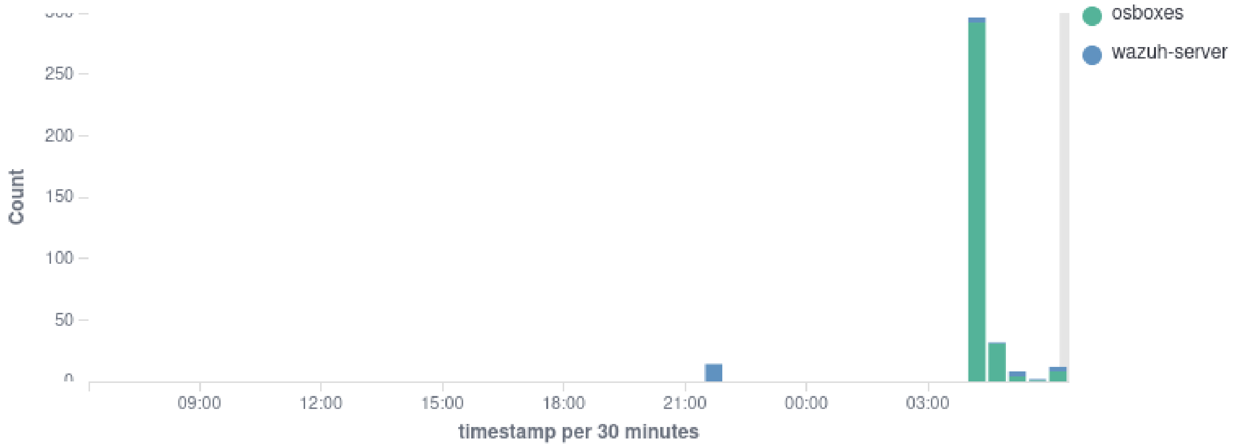
🕘 2025-06-13T06:16:09 to 2025-06-14T06:16:09

🔍 manager.name: wazuh-server

Top 10 Alert level evolution



Alerts evolution - Top 5 agents



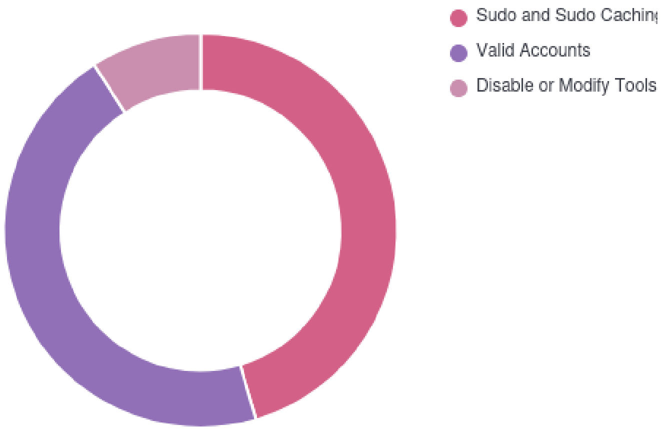
364
- Total -

0
- Level 12 or above alerts -

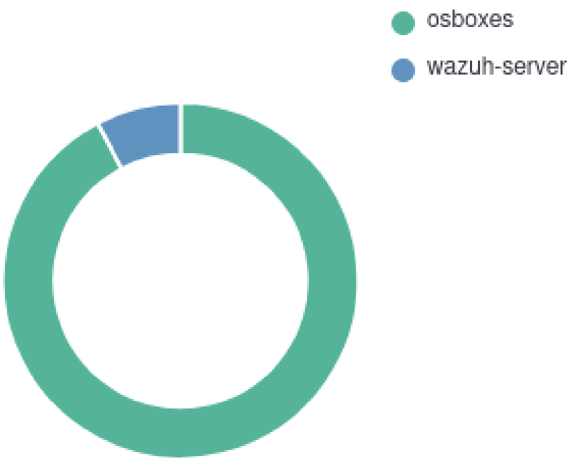
0
- Authentication failure -

5
- Authentication success -

Top 10 MITRE ATT&CKS



Top 5 agents



Alerts summary

Rule ID	Description	Level	Count
533	Listened ports status (netstat) changed (new port opened or closed).	7	12
52002	Apparmor DENIED	3	9
2902	New dpkg (Debian Package) installed.	7	8
2904	Dpkg (Debian Package) half configured.	7	8
80730	Auditd: SELinux permission check.	3	8
2901	New dpkg (Debian Package) requested to install.	3	6
5502	PAM: Login session closed.	3	6
502	Wazuh server started.	3	5
5501	PAM: Login session opened.	3	5
5402	Successful sudo to ROOT executed.	3	4
19004	SCA summary: CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Score less than 50% (40)	7	2
40704	Systemd: Service exited due to a failure.	5	2
52000	Apparmor messages grouped.	3	2
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure /tmp is a separate partition.	7	1
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure AIDE is installed.	7	1
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure AppArmor is enabled in the bootloader configuration.	7	1
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure AppArmor is installed.	7	1
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure Automatic Error Reporting is not enabled.	7	1
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure GDM is removed.	7	1
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure GDM login banner is configured.	7	1
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure X window server services are not in use.	7	1
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure a nftables table exists.	7	1
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure access to all logfiles has been configured.	7	1
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure access to bootloader config is configured.	7	1
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure access to the su command is restricted.	7	1
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure all AppArmor Profiles are enforcing.	7	1
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure all AppArmor Profiles are in enforce or complain mode.	7	1
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure at is restricted to authorized users.	7	1
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure audit tools group owner is configured.	7	1
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure audit tools owner is configured.	7	1
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure audit_backlog_limit is sufficient.	7	1
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure auditd packages are installed.	7	1
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure auditd service is enabled and active.	7	1
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure /dev/shm is a separate partition.	3	1
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure /etc/shadow password fields are not empty.	3	1
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure NIS Client is not installed.	3	1
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure XDMCP is not enabled.	3	1
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure a single firewall configuration utility is in use.	3	1
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure access to /etc/issue is configured.	3	1

Rule ID	Description	Level	Count
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure access to /etc/issue.net is configured.	3	1
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure access to /etc/motd is configured.	3	1
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure accounts in /etc/passwd use shadowed passwords.	3	1
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure address space layout randomization is enabled.	3	1
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure all groups in /etc/passwd exist in /etc/group.	3	1
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure audit configuration files group owner is configured.	3	1
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure audit configuration files mode is configured.	3	1
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure audit configuration files owner is configured.	3	1
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure audit tools mode is configured.	3	1
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure autofs services are not in use.	3	1
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure bluetooth services are not in use.	3	1
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure bogus icmp responses are ignored.	3	1
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure broadcast icmp requests are ignored.	3	1
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure chrony is configured with authorized timeserver.	3	1
19009	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure sudo is installed.	3	1
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure GDM automatic mounting of removable media is disabled.	3	1
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure GDM autorun-never is enabled.	3	1
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure GDM autorun-never is not overridden.	3	1
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure GDM disable-user-list option is enabled.	3	1
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure GDM disabling automatic mounting of removable media is not overridden.	3	1
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure GDM screen locks cannot be overridden.	3	1
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure actions as another user are always logged.	3	1
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure audit log files group owner is configured.	3	1
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure audit log storage size is configured.	3	1
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure audit logs are not automatically deleted.	3	1
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure changes to system administration scope (sudoers) is collected.	3	1
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure cryptographic mechanisms are used to protect the integrity of audit tools.	3	1
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure default user umask is configured.	3	1
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure discretionary access control permission modification events are collected.	3	1
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure events that modify date and time information are collected.	3	1
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure events that modify the sudo log file are collected.	3	1
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure events that modify the system's Mandatory Access Controls are collected.	3	1
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure events that modify the system's network environment are collected.	3	1
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure events that modify user/group information are collected.	3	1
19004	SCA summary: CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Score less than 50% (43)	7	1
100051	netcat listening for incoming connection.	7	1
19012	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure sudo is installed.: Status changed from passed to 'not applicable'	5	1

Rule ID	Description	Level	Count
501	New wazuh agent connected.	3	1
503	Wazuh agent started.	3	1
506	Wazuh agent stopped.	3	1
5403	First time user executed sudo.	4	1