

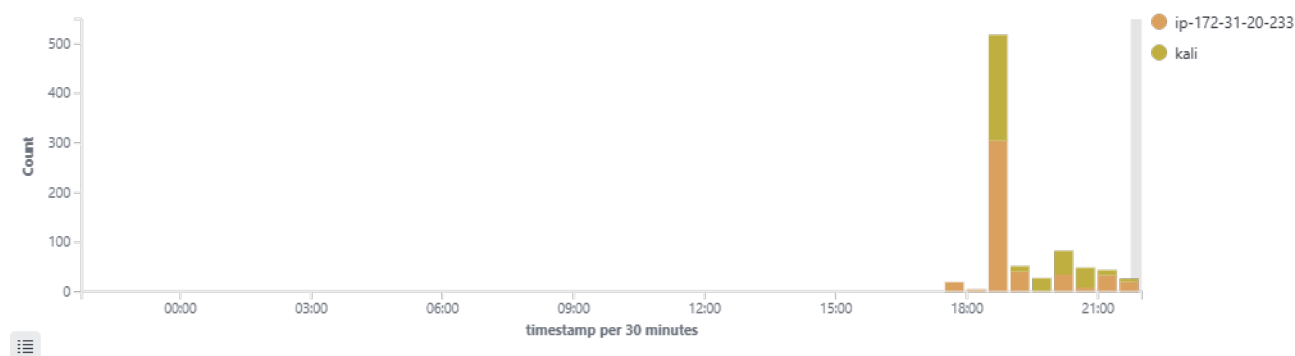
## Security events report

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

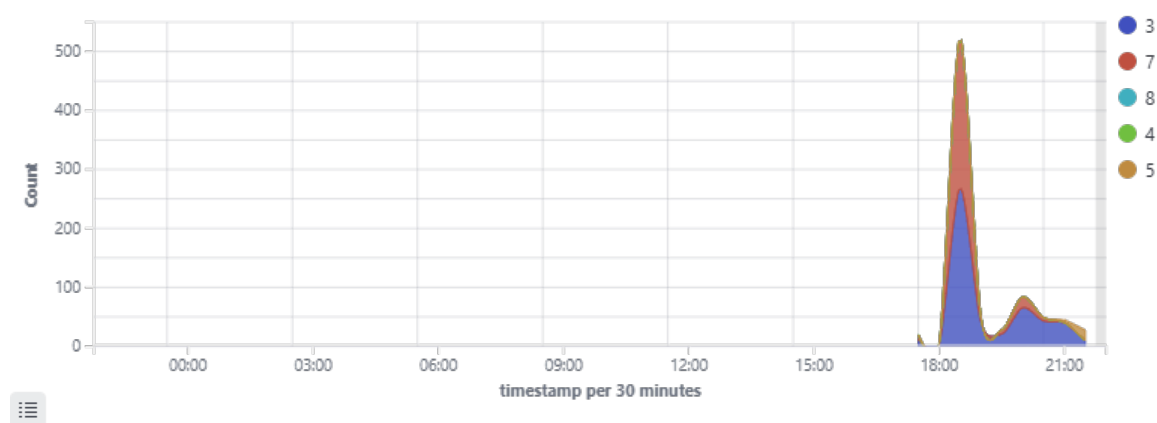
🕒 2025-08-07T21:45:09 to 2025-08-08T21:45:09

🔍 manager.name: ip-172-31-20-233

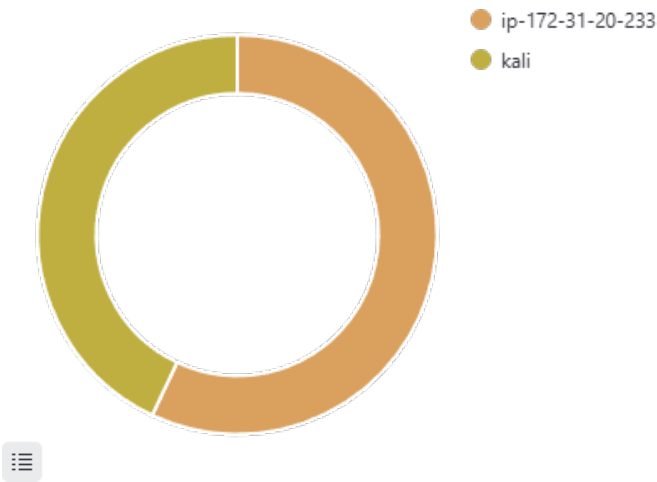
### Alerts evolution Top 5 agents



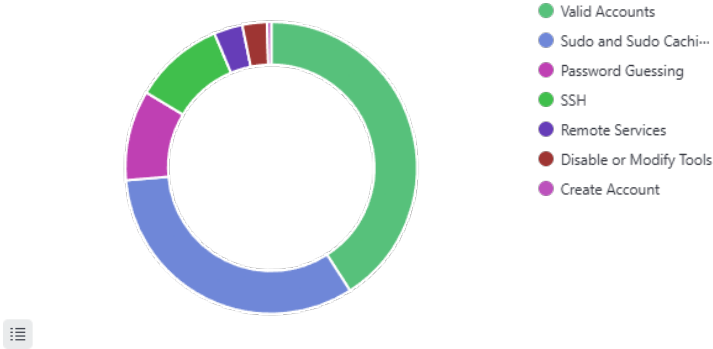
### Alert level evolution



Top 5 agents



Alerts



## Alerts summary

Rule ID	Description	Level	Count
5502	PAM: Login session closed.	3	86
5501	PAM: Login session opened.	3	83
5402	Successful sudo to ROOT executed.	3	69
510	Host-based anomaly detection event (rootcheck).	7	50
5710	sshd: Attempt to login using a non-existent user	5	22
503	Wazuh agent started.	3	7
5715	sshd: authentication success.	3	7
506	Wazuh agent stopped.	3	6
502	Wazuh server started.	3	5
531	Partition usage reached 100% (disk space monitor).	7	4
533	Listened ports status (netstat) changed (new port opened or closed).	7	3
5403	First time user executed sudo.	4	3
19004	SCA summary: CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Score less than 50% (41)	7	2
2901	New dpkg (Debian Package) requested to install.	3	2
2902	New dpkg (Debian Package) installed.	7	2
2904	Dpkg (Debian Package) half configured.	7	2
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Disable USB Storage.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure /etc/hosts.deny is configured.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure AIDE is installed.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure Avahi Server is not enabled.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DCCP is disabled.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure ICMP redirects are not accepted.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 default deny firewall policy.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 loopback traffic is configured.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 router advertisements are not accepted.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure RDS is disabled.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure Reverse Path Filtering is enabled.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SCTP is disabled.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SELinux is not disabled in bootloader configuration.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH AllowTcpForwarding is disabled.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH Idle Timeout Interval is configured.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH LoginGraceTime is set to one minute or less.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxAuthTries is set to 4 or less.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxSessions is set to 4 or less.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxStartups is configured.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH X11 forwarding is disabled.	7	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Disable Automounting.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure /tmp is configured.	3	1

Rule ID	Description	Level	Count
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure CUPS is not enabled.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DHCP Server is not enabled.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DNS Server is not enabled.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure FTP Server is not enabled.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Proxy Server is not enabled.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP server is not enabled.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IMAP and POP3 server is not enabled.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IP forwarding is disabled.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure LDAP client is not installed.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure LDAP server is not enabled.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure NFS and RPC are not enabled.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure NIS Client is not installed.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure NIS Server is not enabled.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SELinux or AppArmor are installed.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SETroubleshoot is not installed.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SNMP Server is not enabled.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH HostbasedAuthentication is disabled.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH IgnoreRhosts is enabled.	3	1
19009	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure AppArmor is not disabled in bootloader configuration.	3	1
19009	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure GDM login banner is configured.	3	1
19009	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SELinux policy is configured.	3	1
19009	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure TCP Wrappers is installed.	3	1
19009	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure password creation requirements are configured.	3	1
19009	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure password hashing algorithm is SHA-512.	3	1
19009	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure password reuse is limited.	3	1
19009	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure the SELinux state is enforcing.	3	1
19009	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure the audit configuration is immutable.	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 login banner is configured.	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
19004	SCA summary: CIS Distribution Independent Linux Benchmark v2.0.0.: Score less than 50% (46)	7	1
501	New wazuh agent connected.	3	1

Rule ID	Description	Level	Count
5901	New group added to the system.	8	1
5902	New user added to the system.	8	1