Security events report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
001	ubuntu_agent	192.168.142.130	Wazuh v4.7.5	siem	Ubuntu 22.04.5 LTS	Dec 2, 2025 @ 07:26:10.000	Dec 2, 2025 @ 08:12:17.000

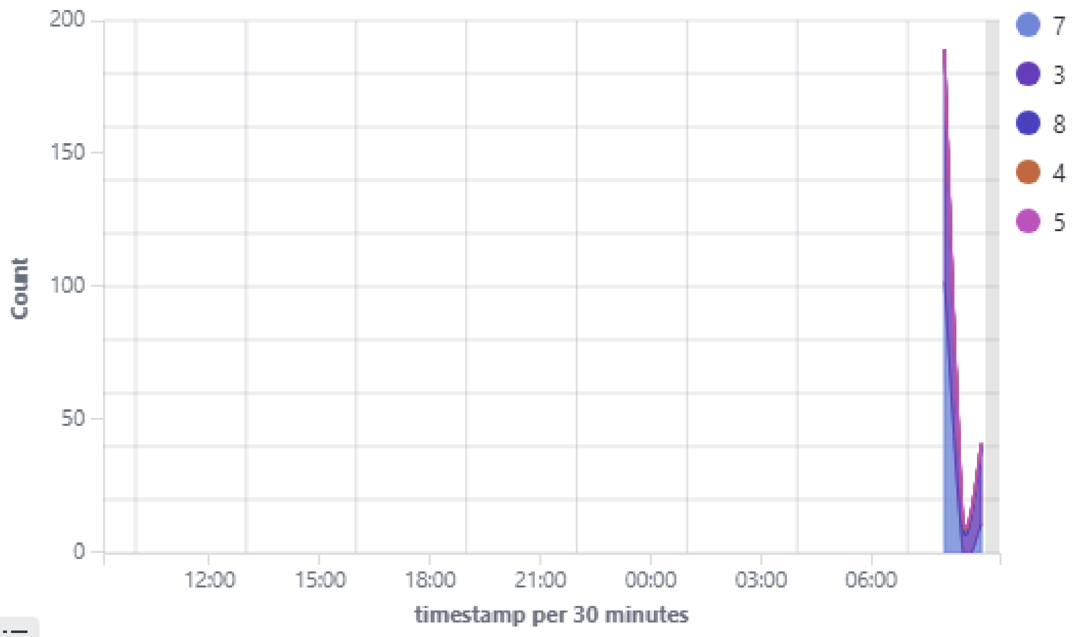
Group: default

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

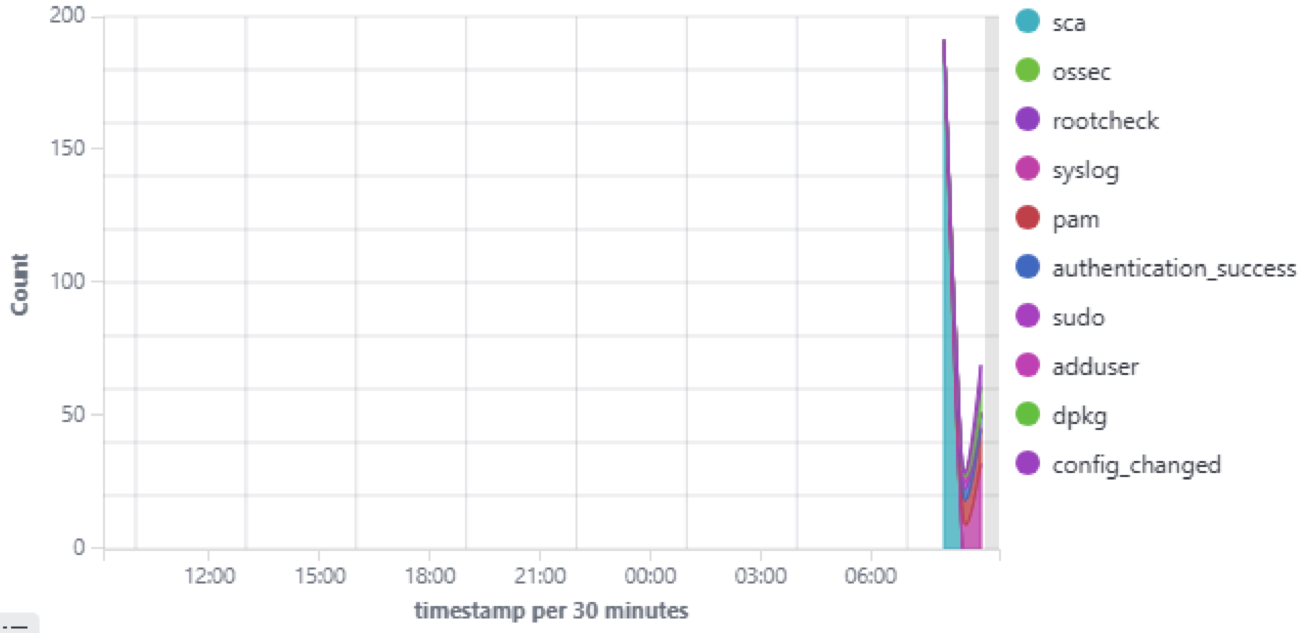
2025-12-01T09:12:15 to 2025-12-02T09:12:15

manager.name: siem AND agent.id: 001

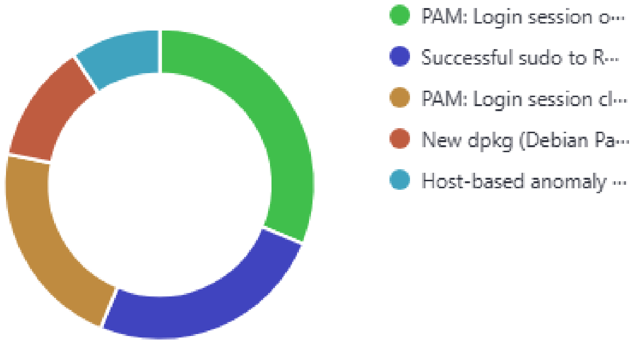
Alerts



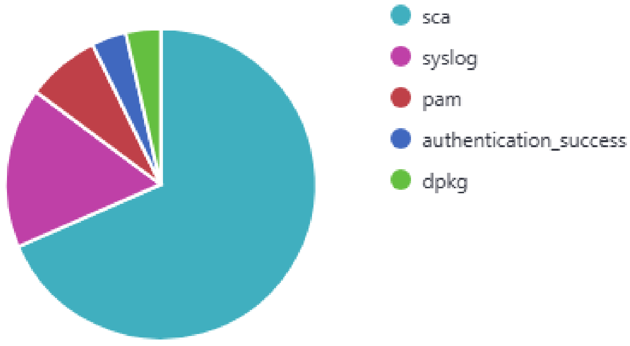
Alert groups evolution



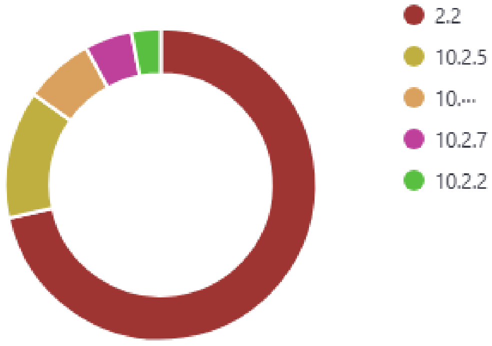
Top 5 alerts



Top 5 rule groups



Top 5 PCI DSS requirements



Alerts summary

Rule ID	Description	Level	Count
5501	PAM: Login session opened.	3	11
5502	PAM: Login session closed.	3	9
5402	Successful sudo to ROOT executed.	3	8
2902	New dpkg (Debian Package) installed.	7	4
2904	Dpkg (Debian Package) half configured.	7	4
510	Host-based anomaly detection event (rootcheck).	7	4
19004	SCA summary: CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Score less than 50% (39)	7	2
2901	New dpkg (Debian Package) requested to install.	3	2
503	Wazuh agent started.	3	2
506	Wazuh agent stopped.	3	2
5555	PAM: User changed password.	3	2
5901	New group added to the system.	8	2
5902	New user added to the system.	8	2
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure /tmp is a separate partition.	7	1
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure AIDE is installed.	7	1
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure AppArmor is enabled in the bootloader configuration.	7	1
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure Automatic Error Reporting is not enabled.	7	1
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure Avahi Server is not installed.	7	1
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure CUPS is not installed.	7	1
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure GNOME Display Manager is removed.	7	1
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure X Window System is not installed.	7	1
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure access to the su command is restricted.	7	1
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure actions as another user are always logged.	7	1
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure all AppArmor Profiles are enforcing.	7	1
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure at is restricted to authorized users.	7	1
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure audit log storage size is configured.	7	1
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure audit logs are not automatically deleted.	7	1
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure audit tools are 755 or more restrictive.	7	1
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure audit tools are owned by root.	7	1
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure audit_backlog_limit is sufficient.	7	1
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure auditd is installed.	7	1
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure auditd service is enabled and active.	7	1
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure auditing for processes that start prior to auditd is enabled.	7	1
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Disable Automounting.	3	1
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure /etc/shadow password fields are not empty.	3	1
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure AppArmor is installed.	3	1
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure DHCP Server is not installed.	3	1
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure DNS Server is not installed.	3	1

Rule ID	Description	Level	Count
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure FTP Server is not installed.	3	1
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure HTTP Proxy Server is not installed.	3	1
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure HTTP server is not installed.	3	1
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure IMAP and POP3 server are not installed.	3	1
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure LDAP client is not installed.	3	1
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure LDAP server is not installed.	3	1
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure NFS is not installed.	3	1
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure NIS Client is not installed.	3	1
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure NIS Server is not installed.	3	1
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure RPC is not installed.	3	1
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure SNMP Server is not installed.	3	1
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure Samba is not installed.	3	1
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure XDCMP is not enabled.	3	1
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure a nftables table exists.	3	1
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure accounts in /etc/passwd use shadowed passwords.	3	1
19009	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure SSH AllowTcpForwarding is disabled.	3	1
19009	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure SSH HostbasedAuthentication is disabled.	3	1
19009	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure SSH Idle Timeout Interval is configured.	3	1
19009	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure SSH IgnoreRhosts is enabled.	3	1
19009	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure SSH LogLevel is appropriate.	3	1
19009	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure SSH LoginGraceTime is set to one minute or less.	3	1
19009	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure SSH MaxAuthTries is set to 4 or less.	3	1
19009	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure SSH MaxSessions is set to 10 or less.	3	1
19009	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure SSH MaxStartups is configured.	3	1
19009	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure SSH PAM is enabled.	3	1
19009	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure SSH PermitEmptyPasswords is disabled.	3	1
19009	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure SSH PermitUserEnvironment is disabled.	3	1
19009	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure SSH X11 forwarding is disabled.	3	1
19009	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure SSH access is limited.	3	1
19009	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure SSH root login is disabled.	3	1
19009	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure SSH warning banner is configured.	3	1
19009	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure ntp access control is configured.	3	1
19009	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure only authorized groups are assigned ownership of audit log files.	3	1
19009	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure only strong Ciphers are used.	3	1
19009	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure only strong Key Exchange algorithms are used.	3	1
19004	SCA summary: CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Score less than 50% (41)	7	1
19010	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure audit log storage size is configured.: Status changed from failed to passed	3	1
19010	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure audit tools are 755 or more restrictive.: Status changed from failed to passed	3	1
19010	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure auditd service is enabled and active.: Status changed from	3	1

Rule ID	Description	Level	Count
	failed to passed		
19015	CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Ensure only authorized groups are assigned ownership of audit log files.: Status changed from 'not applicable' to passed	3	1
2501	syslog: User authentication failure.	5	1
501	New wazuh agent connected.	3	1
5403	First time user executed sudo.	4	1
5903	Group (or user) deleted from the system.	3	1

Groups summary

Groups	Count
sca	189
syslog	47
pam	22
authentication_success	11
dpkg	10
ossec	9
sudo	9
config_changed	8
adduser	5
rootcheck	4
access_control	1
authentication_failed	1