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

Threat hunting report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
002	Debian	192.168.1.148	Wazuh v4.9.2	wazuh-server	Debian GNU/Linux 12	Nov 20, 2024 @ 18:39:55.000	Nov 20, 2024 @ 18:58:15.000

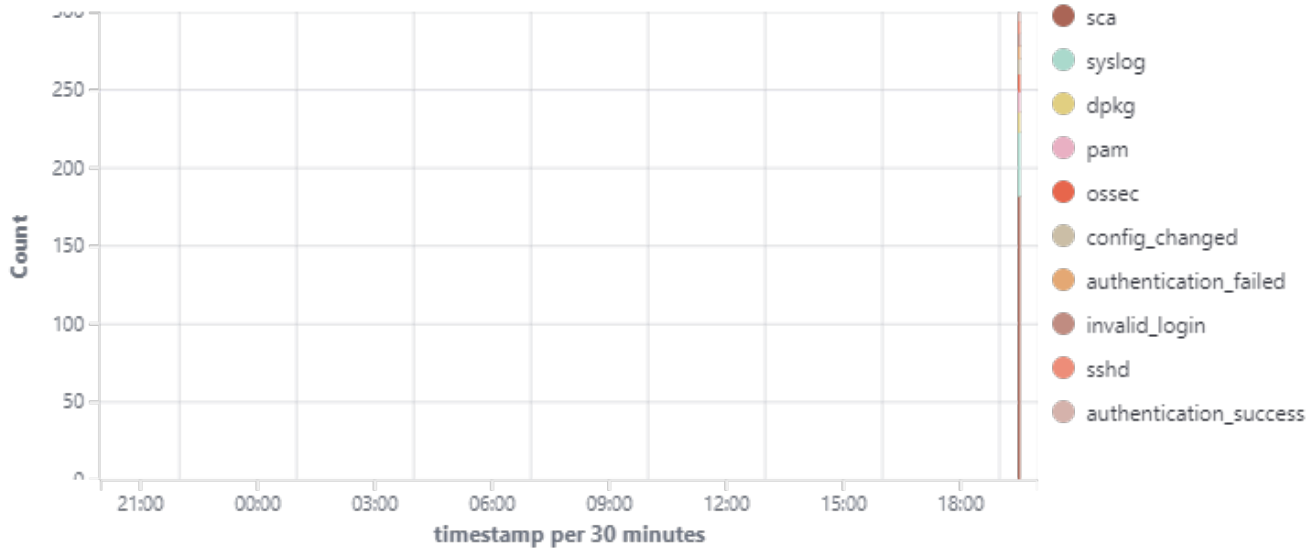
Group: default

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

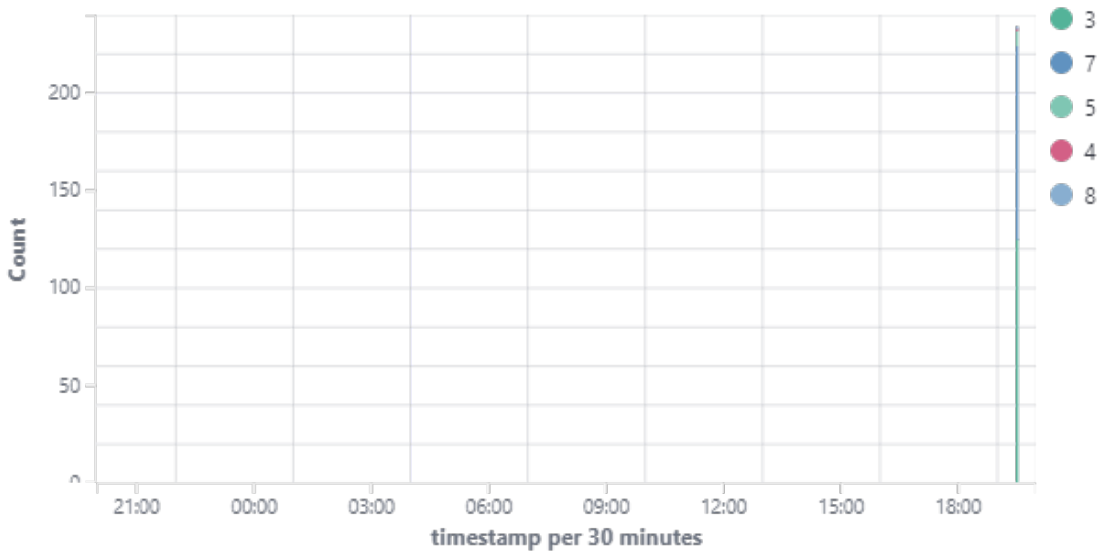
2024-11-19T19:58:23 to 2024-11-20T19:58:23

manager.name: wazuh-server AND agent.id: 002

Top 10 Alert groups evolution



Alerts



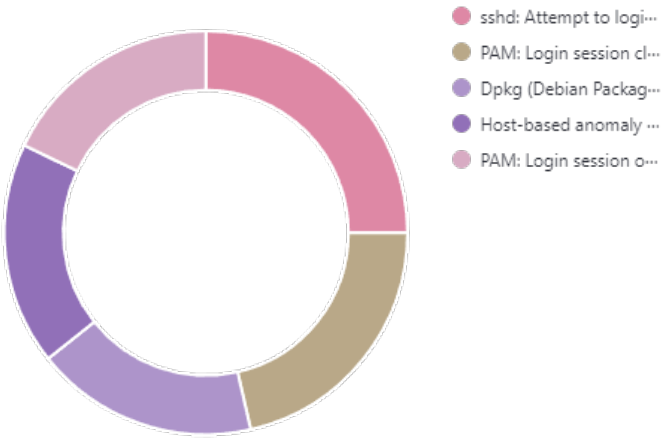
234
- Total -

0
- Level 12 or above alerts -

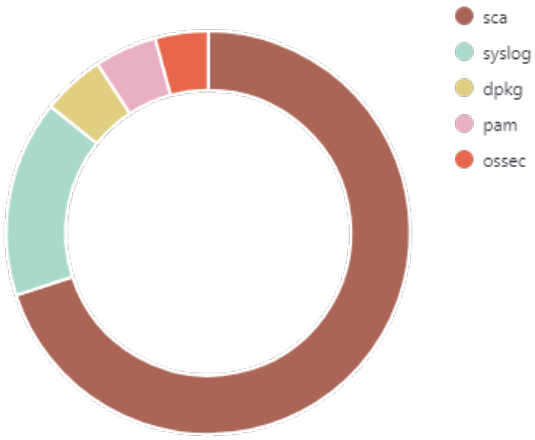
8
- Authentication failure -

6
- Authentication success -

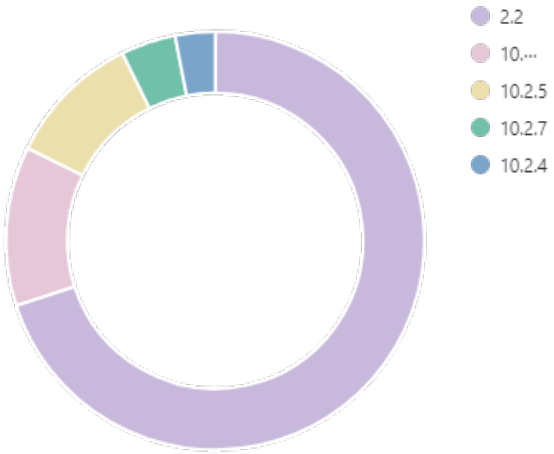
Top 5 alerts



Top 5 rule groups



Top 5 PCI DSS Requirements



Alerts summary

Rule ID	Description	Level	Count
5710	sshd: Attempt to login using a non-existent user	5	8
5502	PAM: Login session closed.	3	7
510	Host-based anomaly detection event (rootcheck).	7	6
5501	PAM: Login session opened.	3	6
2902	New dpkg (Debian Package) installed.	7	5
2904	Dpkg (Debian Package) half configured.	7	5
5402	Successful sudo to ROOT executed.	3	5
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure default deny firewall policy.	7	3
2901	New dpkg (Debian Package) requested to install.	3	3
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure Uncomplicated Firewall is not installed or disabled.	7	2
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure loopback traffic is configured.	7	2
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure NIS Server is not installed.	3	2
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure prelink is disabled.	3	2
503	Wazuh agent started.	3	2
506	Wazuh agent stopped.	3	2
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Disable USB Storage.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure /tmp is configured.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure AIDE is installed.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure AppArmor is enabled in the bootloader configuration.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure Avahi Server is not installed.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure CUPS is not installed.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure DCCP is disabled.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure GDM is removed or login is configured.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure HTTP server is not installed.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure IPv6 default deny firewall policy.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure IPv6 loopback traffic is configured.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure RDS is disabled.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SCTP is disabled.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure TIPC is disabled.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure a table exists.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure access to the su command is restricted.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure accounts in /etc/passwd use shadowed passwords.	7	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Disable Automounting.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure AppArmor is installed.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure DHCP Server is not installed.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure DNS Server is not installed.	3	1

Rule ID	Description	Level	Count
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure FTP Server is not installed.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure HTTP Proxy Server is not installed.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure IMAP and POP3 server are not installed.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure LDAP client is not installed.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure LDAP server is not installed.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure NFS is not installed.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure RPC is not installed.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SNMP Server is not installed.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure Samba is not installed.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure TCP SYN Cookies is enabled.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure Uncomplicated Firewall is installed.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure X Window System is not installed.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure XD/NX support is enabled.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure address space layout randomization (ASLR) is enabled.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH AllowTcpForwarding is disabled.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH HostbasedAuthentication is disabled.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH Idle Timeout Interval is configured.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH IgnoreRhosts is enabled.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH LogLevel is appropriate.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH LoginGraceTime is set to one minute or less.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH MaxAuthTries is set to 4 or less.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH MaxSessions is limited.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH MaxStartups is configured.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH PAM is enabled.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH PermitEmptyPasswords is disabled.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH PermitUserEnvironment is disabled.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH X11 forwarding is disabled.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH access is limited.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH root login is disabled.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH warning banner is configured.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure audit log storage size is configured.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure audit logs are not automatically deleted.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure changes to system administration scope (sudoers) is collected.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure discretionary access control permission modification events are collected.	3	1
19004	SCA summary: Center for Internet Security Debian Family Linux Benchmark v1.0.0: Score less than 50% (43)	7	1
501	New wazuh agent connected.	3	1
5403	First time user executed sudo.	4	1
5902	New user added to the system.	8	1

Groups summary

Groups	Count
sca	182
syslog	41
dpkg	13
pam	13
ossec	11
config_changed	10
authentication_failed	8
invalid_login	8
sshd	8
authentication_success	6
rootcheck	6
sudo	6
adduser	1