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

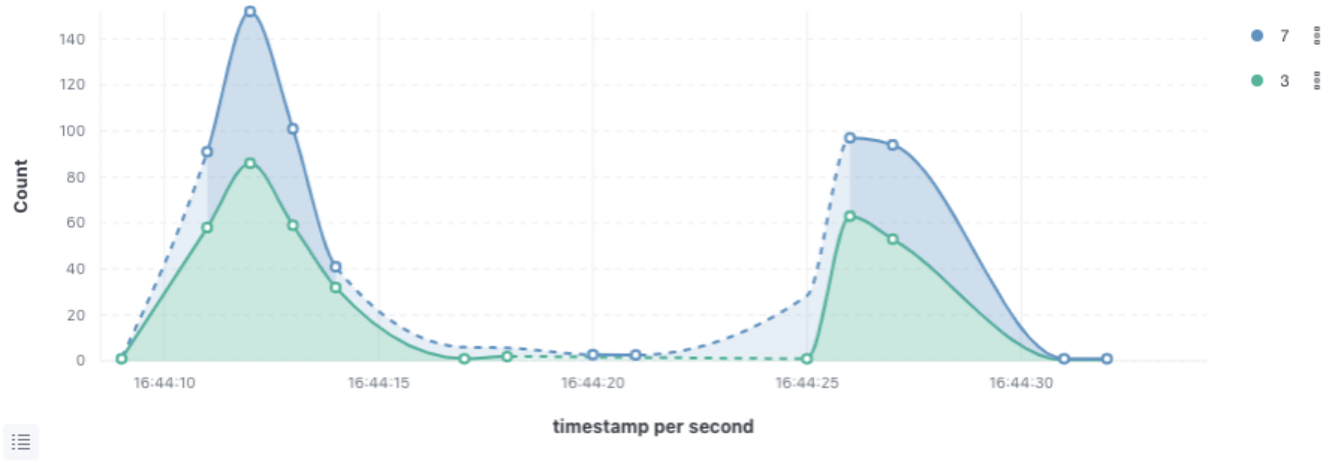
Security events report

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

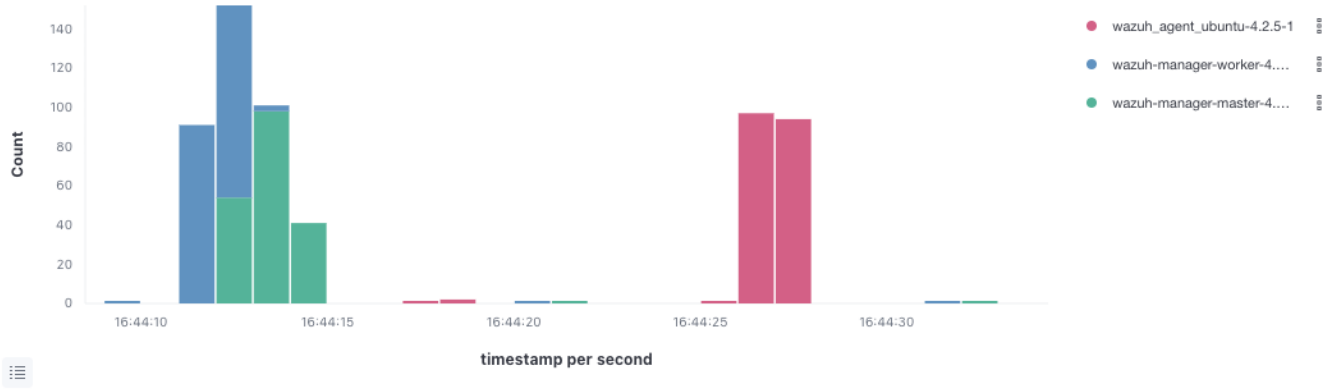
2022-02-16T16:44:08 to 2022-02-16T16:44:34

cluster.name: wazuh

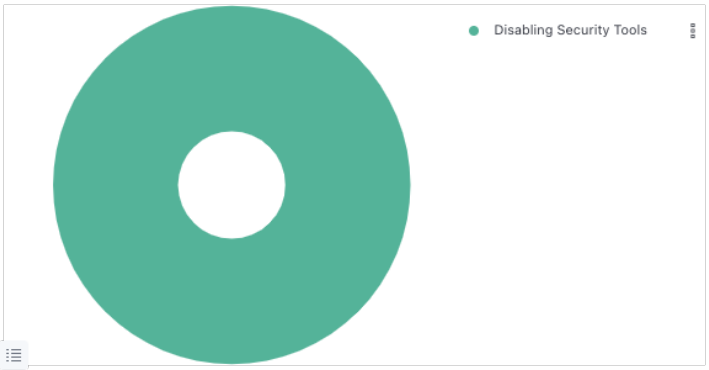
Alert level evolution



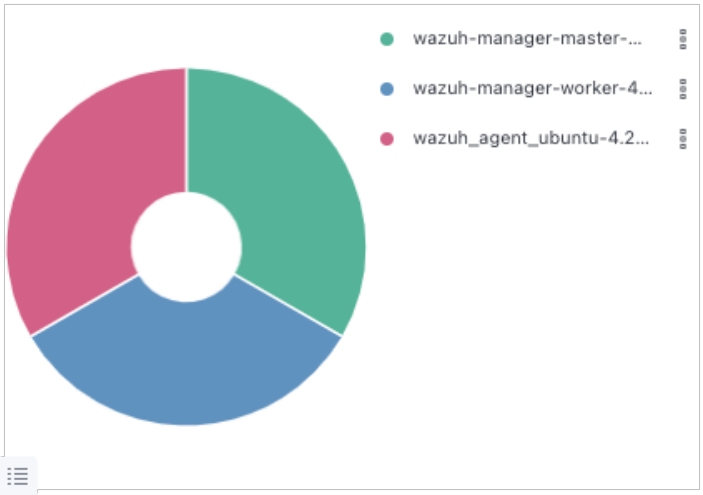
Alerts evolution Top 5 agents



Alerts



Top 5 agents



Alerts summary

Rule ID	Description	Level	Count
19009	CIS Benchmark for Debian/Linux 10: Ensure default deny firewall policy	3	9
19009	CIS Benchmark for Debian/Linux 10: Ensure loopback traffic is configured	3	5
19004	SCA summary: CIS Benchmark for Debian/Linux 10: Score less than 50% (31)	7	4
19009	CIS Benchmark for Debian/Linux 10: Disable Automounting	3	3
19009	CIS Benchmark for Debian/Linux 10: Disable IPv6	3	3
19009	CIS Benchmark for Debian/Linux 10: Disable USB Storage	3	3
19009	CIS Benchmark for Debian/Linux 10: Ensure AppArmor is enabled in the bootloader configuration	3	3
19009	CIS Benchmark for Debian/Linux 10: Ensure Avahi Server is not enabled	3	3
19009	CIS Benchmark for Debian/Linux 10: Ensure CUPS is not enabled	3	3
19009	CIS Benchmark for Debian/Linux 10: Ensure DCCP is disabled	3	3
19009	CIS Benchmark for Debian/Linux 10: Ensure DHCP Server is not enabled	3	3
19009	CIS Benchmark for Debian/Linux 10: Ensure DNS Server is not enabled	3	3
19009	CIS Benchmark for Debian/Linux 10: Ensure FTP Server is not enabled	3	3
19009	CIS Benchmark for Debian/Linux 10: Ensure GDM login banner is configured	3	3
19009	CIS Benchmark for Debian/Linux 10: Ensure HTTP Proxy Server is not enabled	3	3
19009	CIS Benchmark for Debian/Linux 10: Ensure HTTP Server is not enabled	3	3
19009	CIS Benchmark for Debian/Linux 10: Ensure IPv6 default deny firewall policy	3	3
19009	CIS Benchmark for Debian/Linux 10: Ensure IPv6 loopback traffic is configured	3	3
19009	CIS Benchmark for Debian/Linux 10: Ensure LDAP server is not enabled	3	3
19009	CIS Benchmark for Debian/Linux 10: Ensure NFS and RPC are not enabled	3	3
19009	CIS Benchmark for Debian/Linux 10: Ensure NIS Server is not enabled	3	3
19007	CIS Benchmark for Debian/Linux 10: Ensure /tmp is configured	7	3
19007	CIS Benchmark for Debian/Linux 10: Ensure AIDE is installed	7	3
19007	CIS Benchmark for Debian/Linux 10: Ensure AppArmor is installed	7	3
19007	CIS Benchmark for Debian/Linux 10: Ensure ICMP redirects are not accepted	7	3
19007	CIS Benchmark for Debian/Linux 10: Ensure IP forwarding is disabled	7	3
19007	CIS Benchmark for Debian/Linux 10: Ensure IPv6 router advertisements are not accepted	7	3
19007	CIS Benchmark for Debian/Linux 10: Ensure XD/NX support is enabled	7	3
19007	CIS Benchmark for Debian/Linux 10: Ensure a Firewall package is installed	7	3
19007	CIS Benchmark for Debian/Linux 10: Ensure access to the su command is restricted	7	3
19007	CIS Benchmark for Debian/Linux 10: Ensure address space layout randomization (ASLR) is enabled	7	3
19007	CIS Benchmark for Debian/Linux 10: Ensure at/cron is restricted to authorized users	7	3
19007	CIS Benchmark for Debian/Linux 10: Ensure audit log storage size is configured	7	3
19007	CIS Benchmark for Debian/Linux 10: Ensure audit logs are not automatically deleted	7	3
19007	CIS Benchmark for Debian/Linux 10: Ensure auditd is installed	7	3
19007	CIS Benchmark for Debian/Linux 10: Ensure authentication required for single user mode	7	3
19007	CIS Benchmark for Debian/Linux 10: Ensure bogus ICMP responses are ignored	7	3
19007	CIS Benchmark for Debian/Linux 10: Ensure broadcast ICMP requests are ignored	7	3
19007	CIS Benchmark for Debian/Linux 10: Ensure changes to system administration scope (sudoers) is collected	7	3

Rule ID	Description	Level	Count
19007	CIS Benchmark for Debian/Linux 10: Ensure core dumps are restricted	7	3
19007	CIS Benchmark for Debian/Linux 10: Ensure default user shell timeout is 900 seconds or less	7	3
19008	CIS Benchmark for Debian/Linux 10: Ensure LDAP client is not installed	3	3
19008	CIS Benchmark for Debian/Linux 10: Ensure NIS Client is not installed	3	3
19008	CIS Benchmark for Debian/Linux 10: Ensure Reverse Path Filtering is enabled	3	3
19008	CIS Benchmark for Debian/Linux 10: Ensure TCP SYN Cookies is enabled	3	3
19008	CIS Benchmark for Debian/Linux 10: Ensure default group for the root account is GID 0	3	3
19008	CIS Benchmark for Debian/Linux 10: Ensure default user umask is 027 or more restrictive	3	3
19008	CIS Benchmark for Debian/Linux 10: Ensure message of the day is configured properly	3	3
19008	CIS Benchmark for Debian/Linux 10: Ensure no legacy "+" entries exist in /etc/group	3	3
19008	CIS Benchmark for Debian/Linux 10: Ensure no legacy "+" entries exist in /etc/passwd	3	3
19008	CIS Benchmark for Debian/Linux 10: Ensure no legacy "+" entries exist in /etc/shadow	3	3
19008	CIS Benchmark for Debian/Linux 10: Ensure nodev option set on /dev/shm partition	3	3
19008	CIS Benchmark for Debian/Linux 10: Ensure noexec option set on /dev/shm partition	3	3
19008	CIS Benchmark for Debian/Linux 10: Ensure nosuid option set on /dev/shm partition	3	3
19008	CIS Benchmark for Debian/Linux 10: Ensure openbsd-inetd is not installed	3	3
19008	CIS Benchmark for Debian/Linux 10: Ensure password expiration warning days is 7 or more	3	3
19008	CIS Benchmark for Debian/Linux 10: Ensure password fields are not empty	3	3
19008	CIS Benchmark for Debian/Linux 10: Ensure password hashing algorithm is SHA-512	3	3
19008	CIS Benchmark for Debian/Linux 10: Ensure password reuse is limited	3	3
19008	CIS Benchmark for Debian/Linux 10: Ensure permissions on /etc/group are configured	3	3
19008	CIS Benchmark for Debian/Linux 10: Ensure permissions on /etc/gshadow are configured	3	3
502	Ossec server started.	3	2
501	New ossec agent connected.	3	1
503	Ossec agent started.	3	1
506	Ossec agent stopped.	3	1