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

Security events report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
003	Web-Server	192.168.1.23	Wazuh v4.5.2	wazuh-server	Ubuntu 18.04.4 LTS	Sep 9, 2023 @ 03:39:26.000	Sep 11, 2023 @ 21:26:22.000

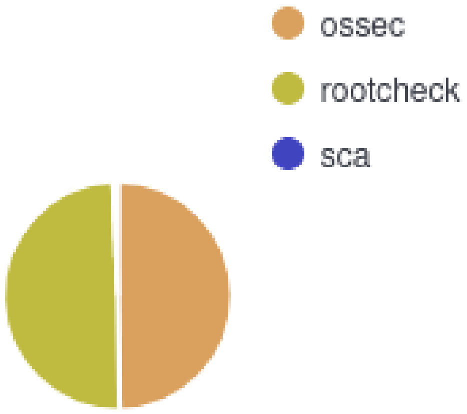
Group: default

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

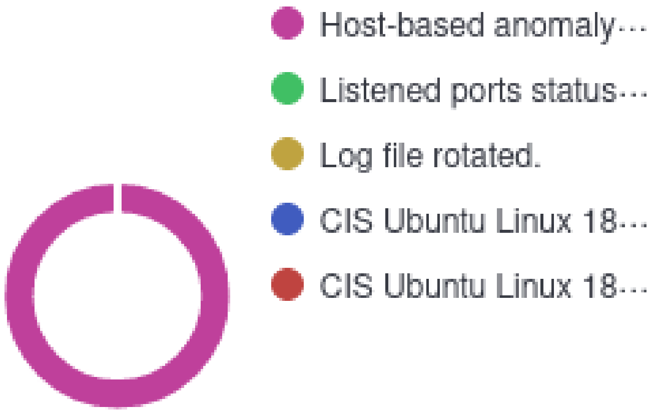
2023-09-04T17:25:49 to 2023-09-11T17:25:49

manager.name: wazuh-server AND agent.id: 003

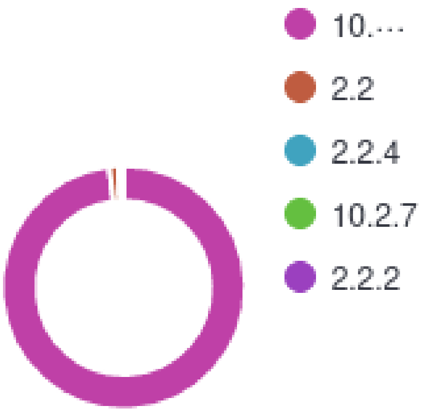
Top 5 rule groups



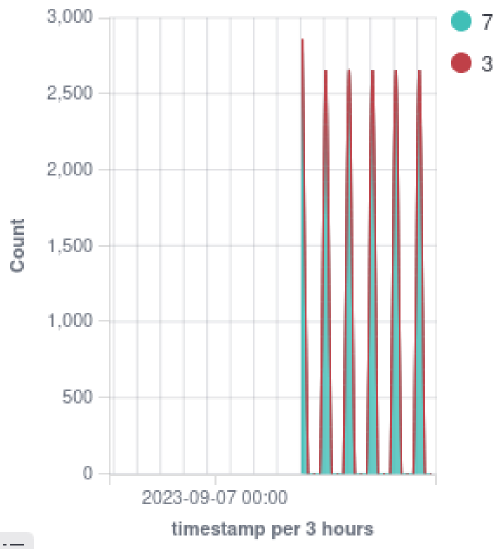
Top 5 alerts



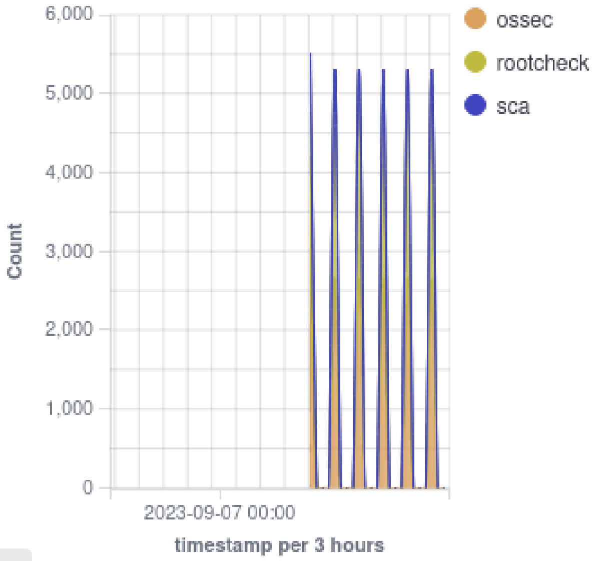
Top 5 PCI DSS requirements



Alerts



Alert groups evolution



Alerts summary

Rule ID	Description	Level	Count
510	Host-based anomaly detection event (rootcheck).	7	15936
533	Listened ports status (netstat) changed (new port opened or closed).	7	22
591	Log file rotated.	3	11
19007	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure default deny firewall policy.	7	2
19007	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure loopback traffic is configured.	7	2
19004	SCA summary: CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Score less than 50% (37)	7	2
19007	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Disable IPv6.	7	1
19007	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Disable USB Storage.	7	1
19007	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure /etc/hosts.deny is configured.	7	1
19007	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure /tmp is configured.	7	1
19007	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure AIDE is installed.	7	1
19007	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure AppArmor is enabled in the bootloader configuration.	7	1
19007	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure DCCP is disabled.	7	1
19007	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure HTTP Server is not enabled.	7	1
19007	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure ICMP redirects are not accepted.	7	1
19007	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure IP forwarding is disabled.	7	1
19007	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure IPv6 default deny firewall policy.	7	1
19007	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure IPv6 loopback traffic is configured.	7	1
19007	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure IPv6 router advertisements are not accepted.	7	1
19007	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure RDS is disabled.	7	1
19007	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure SCTP is disabled.	7	1
19007	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure SSH AllowTcpForwarding is disabled.	7	1
19007	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure SSH Idle Timeout Interval is configured.	7	1
19007	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure SSH LoginGraceTime is set to one minute or less.	7	1
19008	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Disable Automounting.	3	1
19008	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure /etc/hosts.allow is configured.	3	1
19008	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure AppArmor is installed.	3	1
19008	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure Avahi Server is not enabled.	3	1
19008	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure CUPS is not enabled.	3	1
19008	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure DHCP Server is not enabled.	3	1
19008	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure DNS Server is not enabled.	3	1
19008	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure FTP Server is not enabled.	3	1
19008	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure HTTP Proxy Server is not enabled.	3	1
19008	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure LDAP client is not installed.	3	1
19008	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure LDAP server is not enabled.	3	1
19008	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure NFS and RPC are not enabled.	3	1
19008	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure NIS Client is not installed.	3	1
19008	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure NIS Server is not enabled.	3	1
19008	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure Reverse Path Filtering is enabled.	3	1

Rule ID	Description	Level	Count
19008	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure SNMP Server is not enabled.	3	1
19008	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure SSH HostbasedAuthentication is disabled.	3	1
19008	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure SSH IgnoreRhosts is enabled.	3	1
19008	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure SSH LogLevel is appropriate.	3	1
19008	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure SSH PAM is enabled.	3	1
19009	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure GDM login banner is configured.	3	1
19009	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure a table exists.	3	1
19009	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure base chains exist.	3	1
19009	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure chrony is configured.	3	1
19009	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure default deny firewall policy.	3	1
19009	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure ntp is configured.	3	1
19009	CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1: Ensure wireless interfaces are disabled.	3	1
501	New wazuh agent connected.	3	1
503	Wazuh agent started.	3	1

Groups summary

Groups	Count
ossec	15971
rootcheck	15936
sca	200