Security events report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
001	lib-virtual-machine	192.168.57.133	Wazuh v4.7.2	random-virtual-machine	Ubuntu 22.04.4 LTS	Feb 29, 2024 @ 03:04:54.000	Mar 2, 2024 @ 20:30:33.000

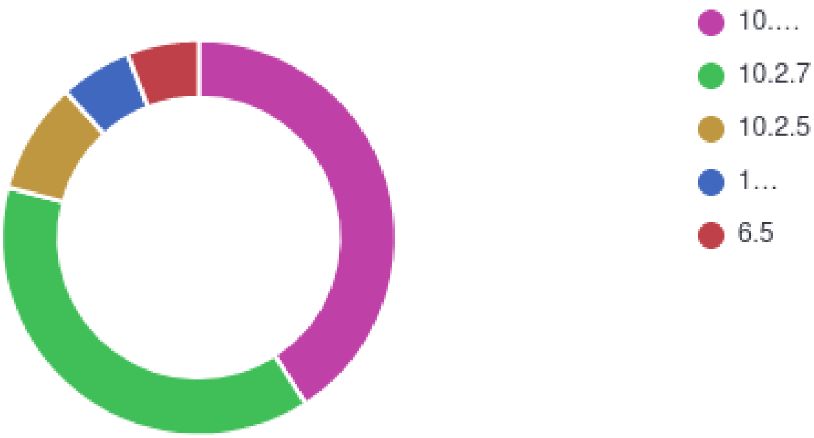
Group: default

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

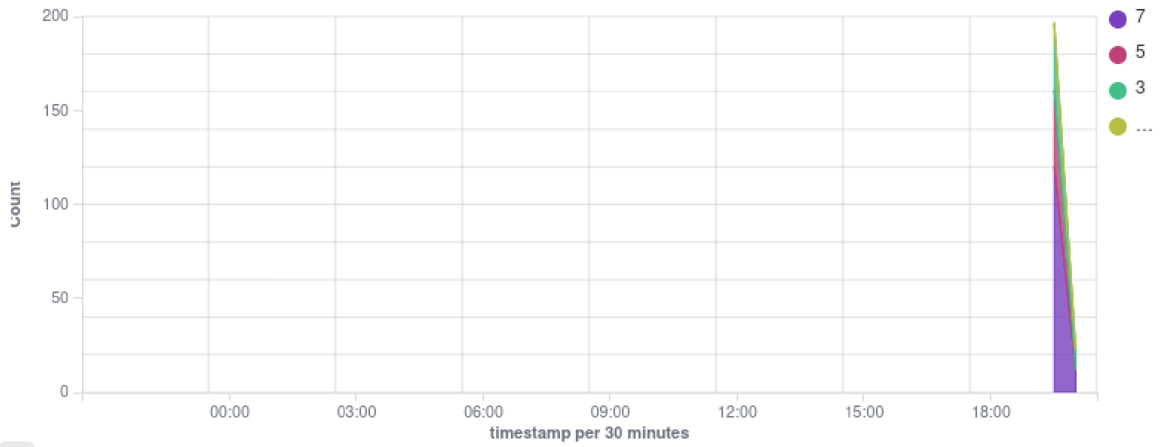
2024-03-01T20:30:37 to 2024-03-02T20:30:37

manager.name: random-virtual-machine AND agent.id: 001

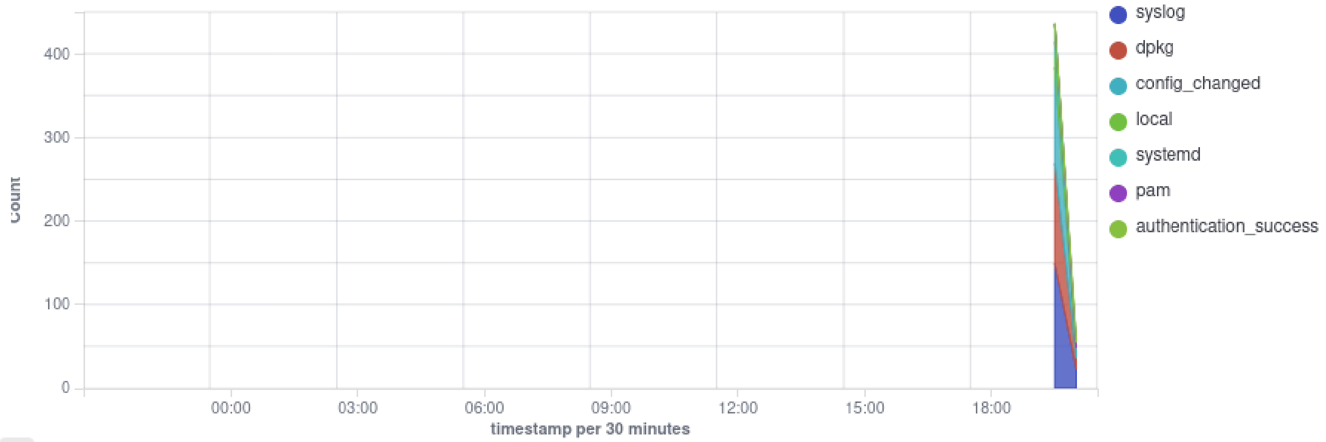
Top 5 PCI DSS requirements



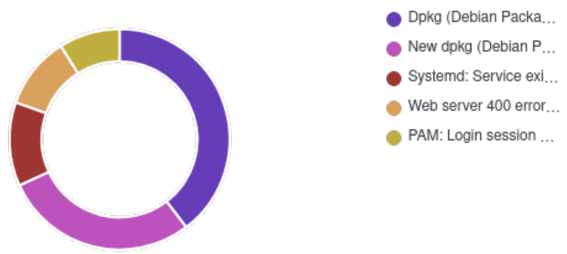
Alerts



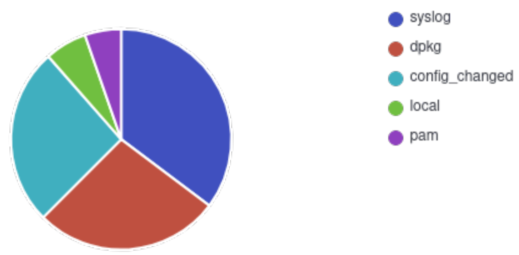
Alert groups evolution



Top 5 alerts



Top 5 rule groups



Alerts summary

Rule ID	Description	Level	Count
2904	Dpkg (Debian Package) half configured.	7	71
2902	New dpkg (Debian Package) installed.	7	51
40704	Systemd: Service exited due to a failure.	5	22
31101	Web server 400 error code.	5	19
5501	PAM: Login session opened.	3	16
5502	PAM: Login session closed.	3	10
52002	Apparmor DENIED	3	8
2901	New dpkg (Debian Package) requested to install.	3	6
2903	Dpkg (Debian Package) removed.	7	5
5402	Successful sudo to ROOT executed.	3	5
533	Listened ports status (netstat) changed (new port opened or closed).	7	3
510	Host-based anomaly detection event (rootcheck).	7	2
31151	Multiple web server 400 error codes from same source ip.	10	1
503	Wazuh agent started.	3	1

Groups summary

Groups	Count
syslog	172
dpkg	133
config_changed	127
local	30
pam	26
systemd	22
accesslog	20
web	20
attack	19
authentication_success	16
apparmor	8
ossec	6
sudo	5
rootcheck	2
recon	1
web_scan	1