Peersoc

Security events report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
001	second_server	167.235.23.58	Wazuh v4.7.5	ubuntu-4gb-nbg1-2	Ubuntu 24.04.1 LTS	Nov 8, 2024 @ 11:02:54.000	Nov 8, 2024 @ 14:33:14.000

Group: default

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

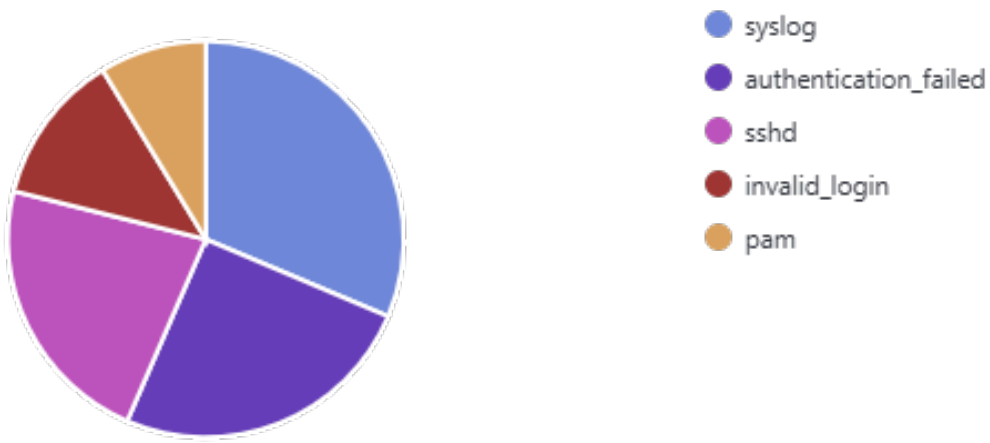
2024-11-07T17:33:14 to 2024-11-08T17:33:14

manager.name: ubuntu-4gb-nbg1-2 AND agent.id: 001

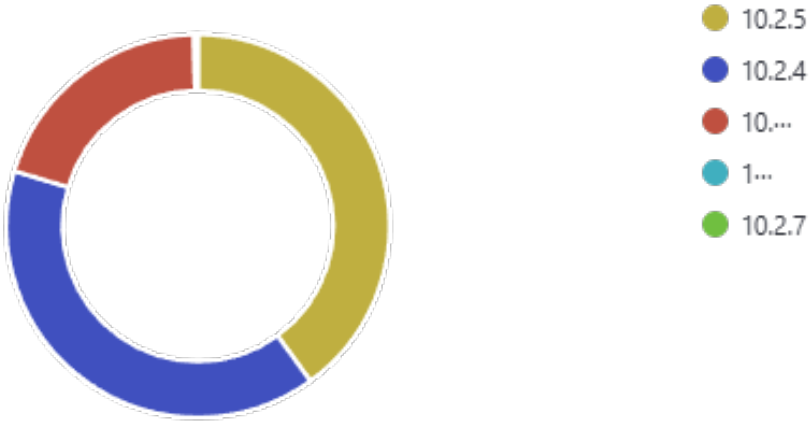
Top 5 alerts

Peersoc

Top 5 rule groups

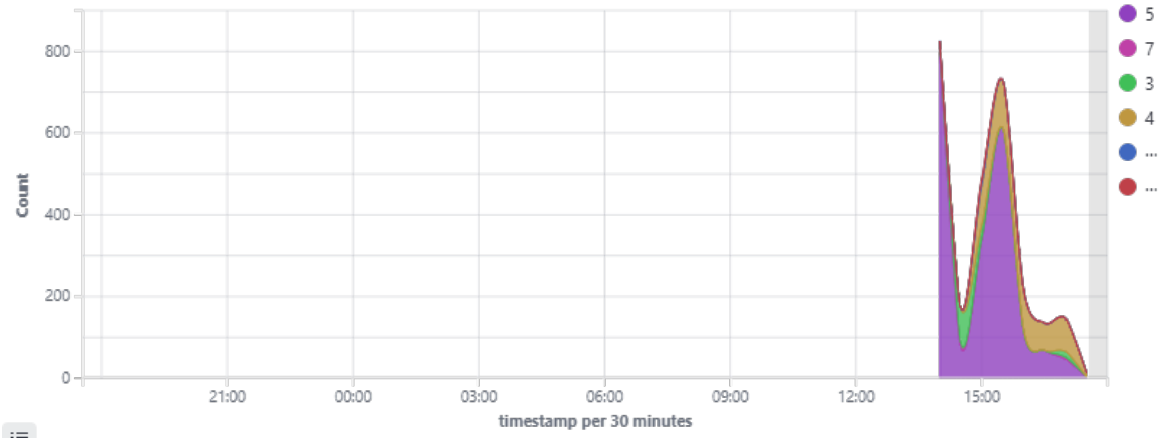


Top 5 PCI DSS requirements

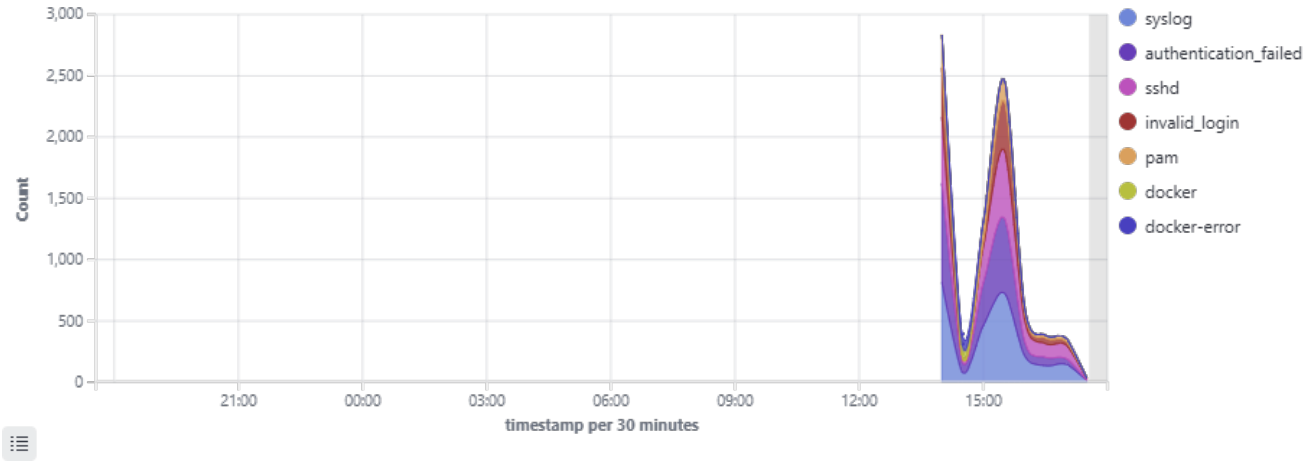


Peersoc

Alerts



Alert groups evolution



Peersoc

Alerts summary

Rule ID	Description	Level	Count
5710	sshd: Attempt to login using a non-existent user	5	1023
5503	PAM: User login failed.	5	701
5760	sshd: authentication failed.	5	346
5762	sshd: connection reset	4	236
5740	sshd: connection reset by peer	4	234
86003	Docker: Error message	3	112
510	Host-based anomaly detection event (rootcheck).	7	18
5501	PAM: Login session opened.	3	8
5502	PAM: Login session closed.	3	8
5712	sshd: brute force trying to get access to the system. Non existent user.	10	8
5108	System running out of memory. Availability of the system is in risk.	12	4
5551	PAM: Multiple failed logins in a small period of time.	10	4
2501	syslog: User authentication failure.	5	3
2502	syslog: User missed the password more than one time	10	3
2904	Dpkg (Debian Package) half configured.	7	3
5402	Successful sudo to ROOT executed.	3	3
5758	Maximum authentication attempts exceeded.	8	3
2902	New dpkg (Debian Package) installed.	7	2
503	Wazuh agent started.	3	2
506	Wazuh agent stopped.	3	2
5715	sshd: authentication success.	3	2
2901	New dpkg (Debian Package) requested to install.	3	1
501	New wazuh agent connected.	3	1
5403	First time user executed sudo.	4	1
5763	sshd: brute force trying to get access to the system. Authentication failed.	10	1

Peersoc

Groups summary

Groups	Count
syslog	2594
authentication_failed	2079
sshd	1853
invalid_login	1023
pam	721
docker	112
docker-error	112
ossec	23
rootcheck	18
authentication_failures	13
authentication_success	10
access_control	6
dpkg	6
config_changed	5
linuxkernel	4
service_availability	4
sudo	4