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

Threat hunting report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
004	debian	192.168.0.23	Wazuh v4.9.2	wazuh-server	Debian GNU/Linux 12	Nov 21, 2024 @ 19:00:59.000	Nov 21, 2024 @ 20:06:55.000

Group: default

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

2024-11-20T18:32:35 to 2024-11-21T18:32:35

manager.name: wazuh-server AND agent.id: 004 AND rule.description: (Web server 400 error code. OR CMS (WordPress or Joomla) login attempt. OR Successful sudo to ROOT executed. OR PAM: User login failed. OR Host-based anomaly detection event (rootcheck). OR Listened ports status (netstat) changed (new port opened or closed). OR unix_chkpwd: Password check failed.)

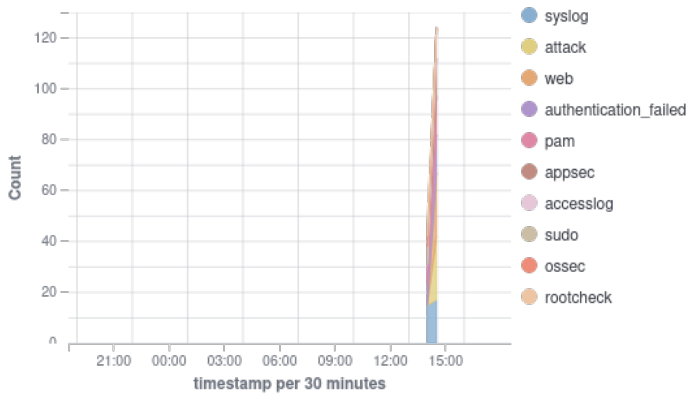
61
- Total -

0
- Level 12 or above alerts -

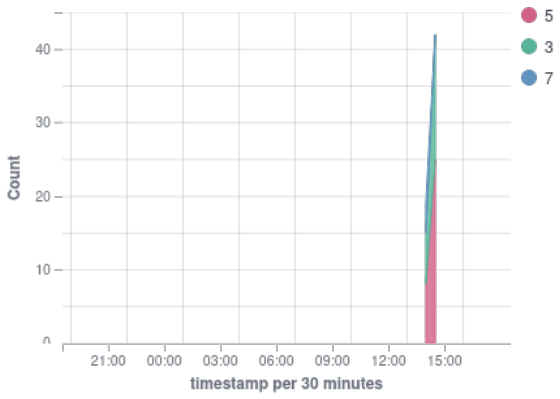
23
- Authentication failure -

0
- Authentication success -

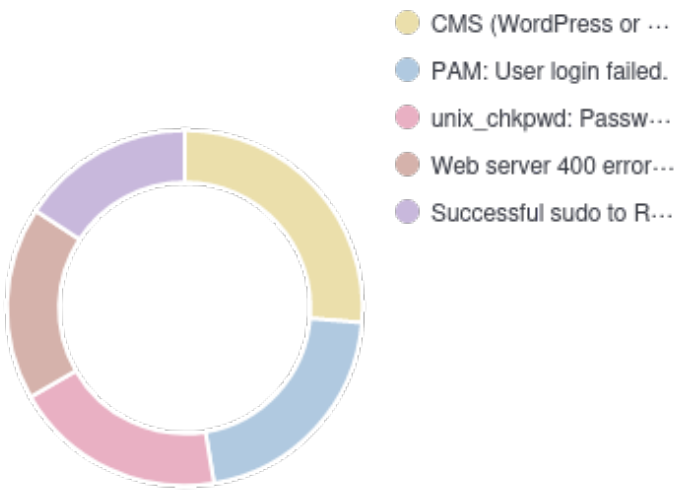
Top 10 Alert groups evolution



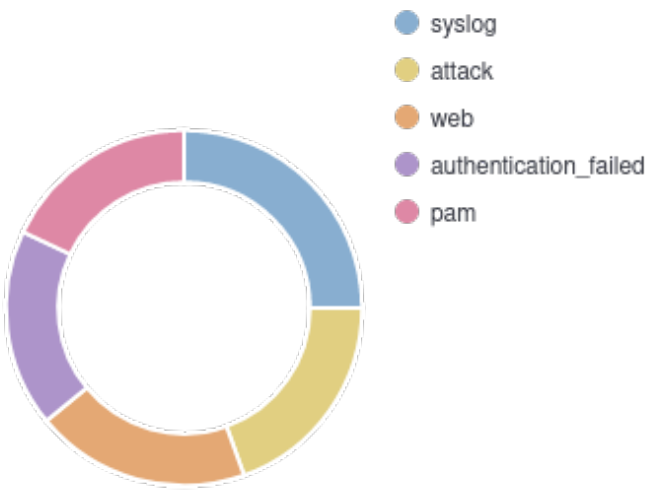
Alerts



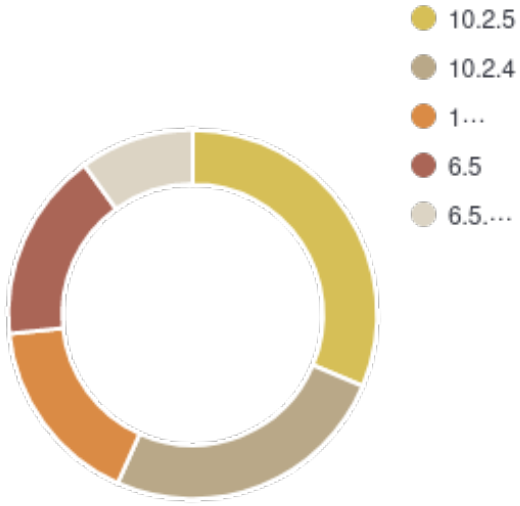
Top 5 alerts



Top 5 rule groups



Top 5 PCI DSS Requirements



Alerts summary

Rule ID	Description	Level	Count
31509	CMS (WordPress or Joomla) login attempt.	3	15
5503	PAM: User login failed.	5	12
5557	unix_chkpwd: Password check failed.	5	11
31101	Web server 400 error code.	5	10
5402	Successful sudo to ROOT executed.	3	9
510	Host-based anomaly detection event (rootcheck).	7	4

Groups summary

Groups	Count
syslog	32
attack	25
web	25
authentication_failed	23
pam	23
appsec	15
accesslog	10
sudo	9
ossec	4
rootcheck	4