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

Threat hunting report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
004	vmware-ubuntu-server	[redacted]	Wazuh v4.14.3	gc-ubuntu	Ubuntu 25.10	Feb 15, 2026 @ 14:37:34.000	Feb 15, 2026 @ 18:45:18.000

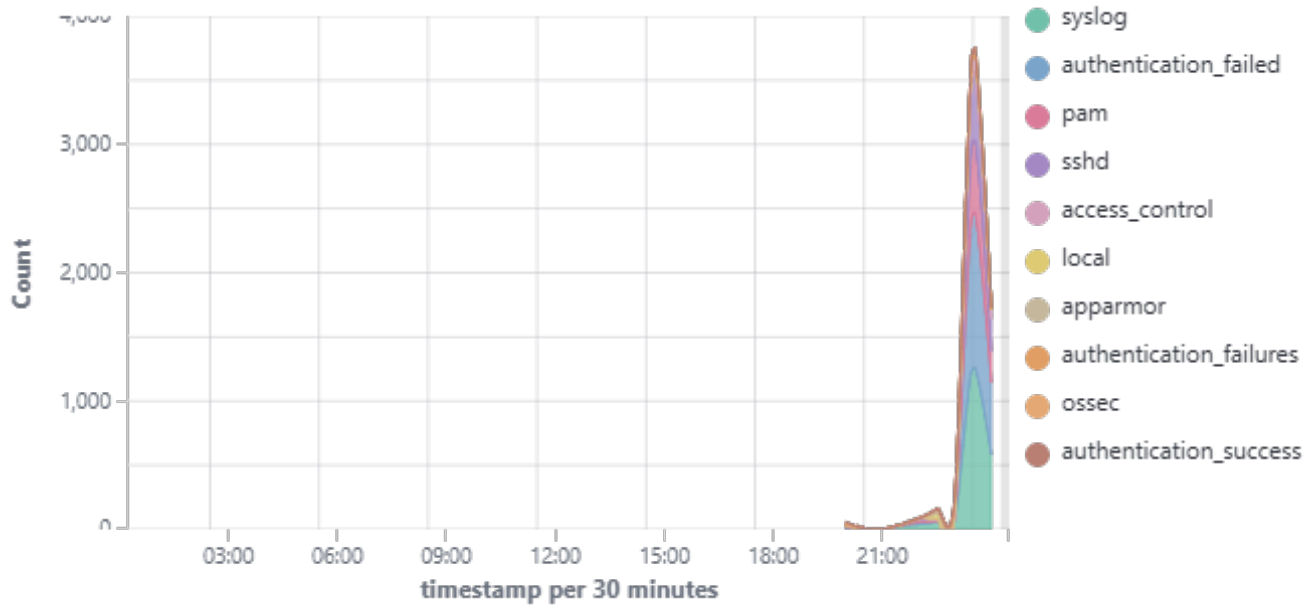
Group: default

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

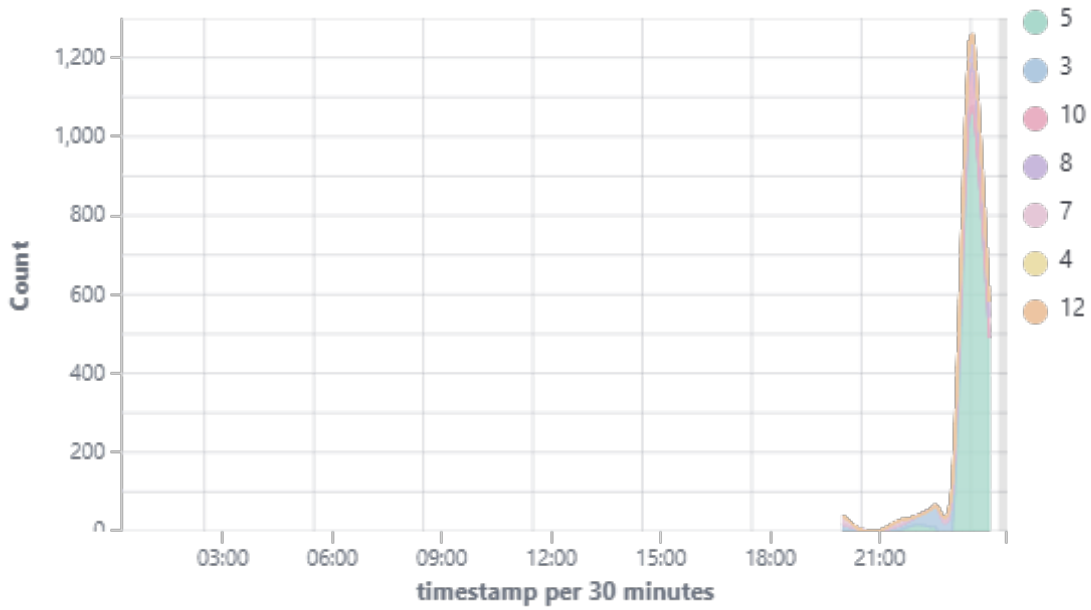
2026-02-15T00:15:36 to 2026-02-16T00:15:36

manager.name: gc-ubuntu AND agent.id: 004

Top 10 Alert groups evolution



Alerts



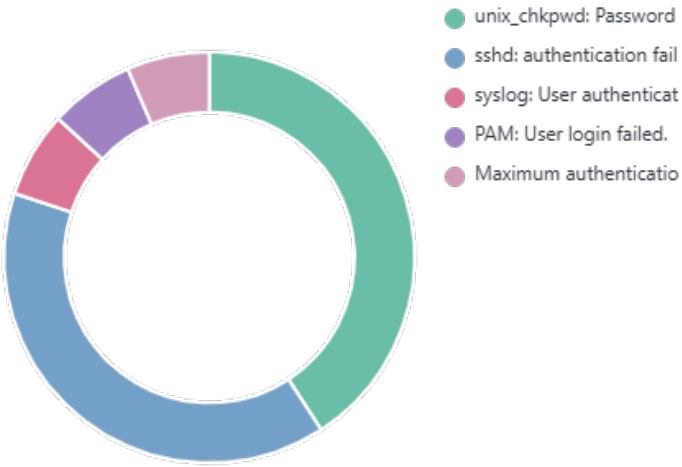
2,140
- Total -

1
- Level 12 or above alerts -

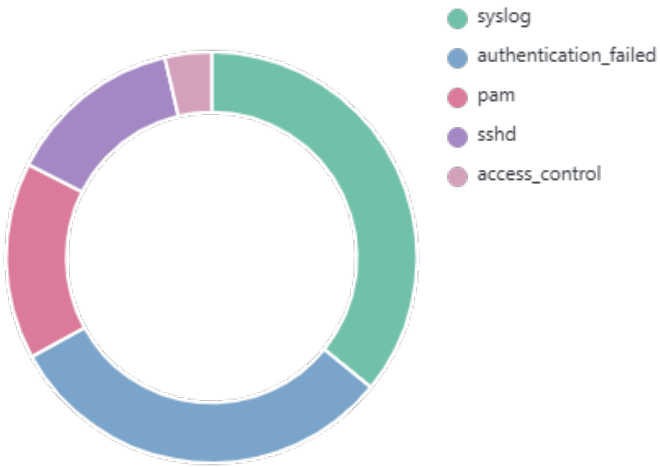
1,860
- Authentication failure -

45
- Authentication success -

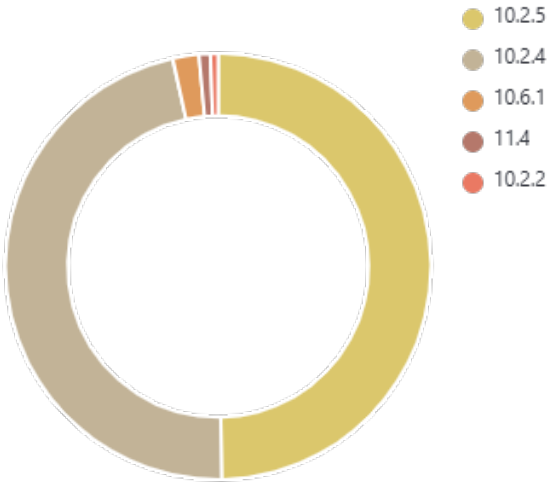
Top 5 alerts



Top 5 rule groups



Top 5 PCI DSS Requirements



Alerts summary

Rule ID	Description	Level	Count
5557	unix_chkpwd: Password check failed.	5	690
5760	sshd: authentication failed.	5	663
2501	syslog: User authentication failure.	5	114
5503	PAM: User login failed.	5	113
5758	Maximum authentication attempts exceeded.	8	110
2502	syslog: User missed the password more than one time	10	98
52002	Apparmor DENIED	3	78
510	Host-based anomaly detection event (rootcheck).	7	44
5501	PAM: Login session opened.	3	44
5502	PAM: Login session closed.	3	33
40111	Multiple authentication failures.	10	30
5402	Successful sudo to ROOT executed.	3	22
40704	Systemd: Service exited due to a failure.	5	17
5763	sshd: brute force trying to get access to the system. Authentication failed.	10	17
5551	PAM: Multiple failed logins in a small period of time.	10	14
52000	Apparmor messages grouped.	3	12
5710	sshd: Attempt to login using a non-existent user	5	11
2902	New dpkg (Debian Package) installed.	7	6
2904	Dpkg (Debian Package) half configured.	7	6
2901	New dpkg (Debian Package) requested to install.	3	4
5555	PAM: User changed password.	3	2
5901	New group added to the system.	8	2
5902	New user added to the system.	8	2
40112	Multiple authentication failures followed by a success.	12	1
501	New wazuh agent connected.	3	1
503	Wazuh agent started.	3	1
506	Wazuh agent stopped.	3	1
5403	First time user executed sudo.	4	1
5715	sshd: authentication success.	3	1
5903	Group (or user) deleted from the system.	3	1
5904	Information from the user was changed.	8	1

Groups summary

Groups	Count
syslog	2076
authentication_failed	1799
pam	896
sshd	802
access_control	212
local	107
apparmor	90
authentication_failures	61
ossec	47
authentication_success	45
rootcheck	44
attacks	31
sudo	23
systemd	17
dpkg	16
config_changed	12
invalid_login	11
adduser	6