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

Threat hunting report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
001	victima	10.128.0.3	Wazuh v4.9.1	instance-20241026-022758	Debian GNU/Linux 12	Oct 28, 2024 @ 03:00:52.000	Nov 5, 2024 @ 18:27:36.000

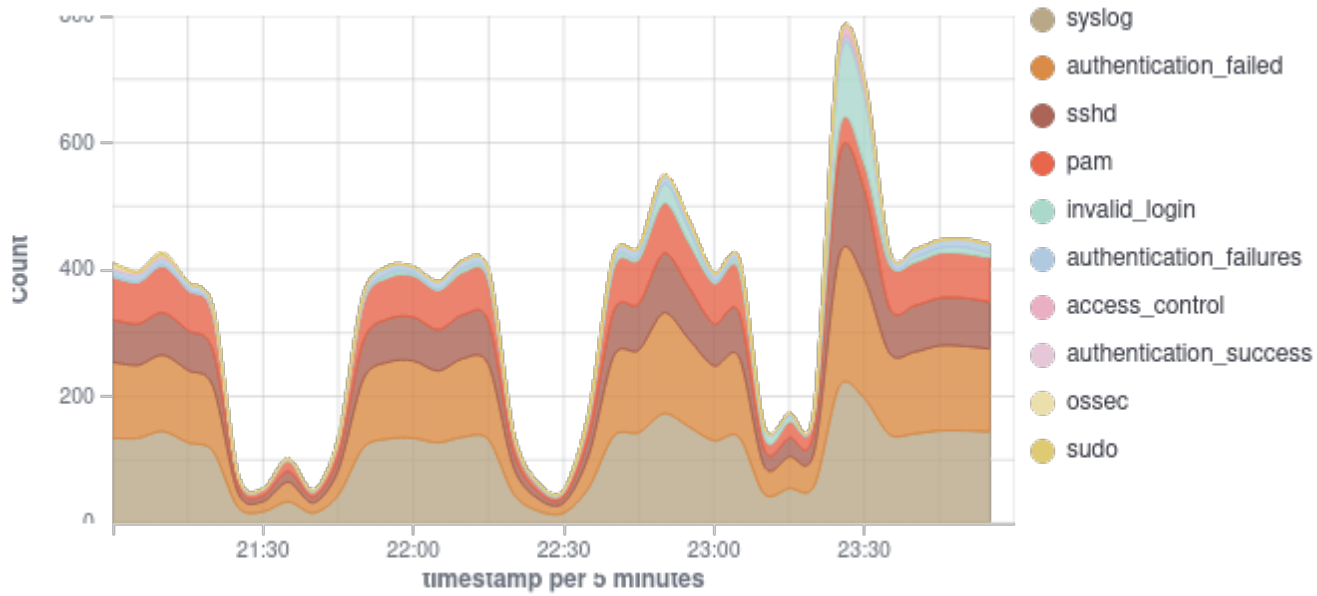
Group: default

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

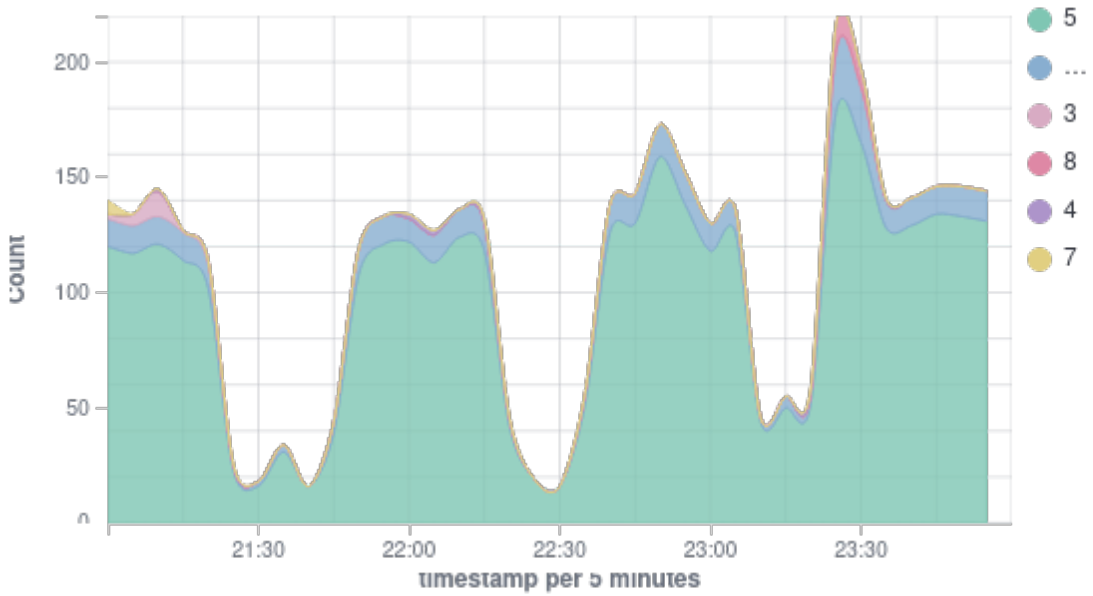
2024-10-30T21:00:00 to 2024-10-31T00:00:00

manager.name: instance-20241026-022758 AND agent.id: 001

Top 10 Alert groups evolution



Alerts



3,879

- Total -

0

- Level 12 or above alerts -

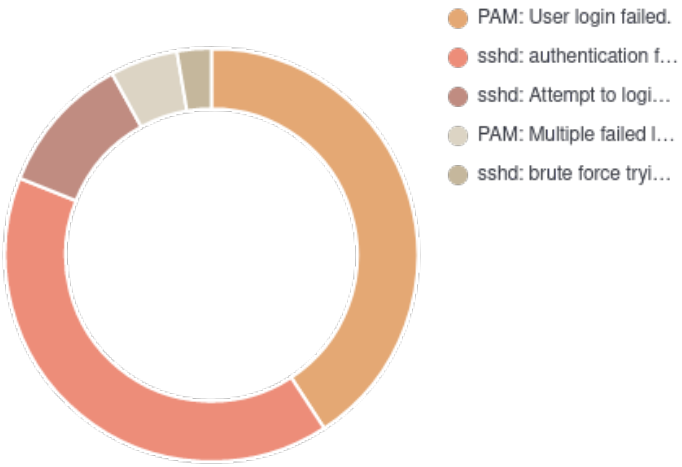
3,836

- Authentication failure -

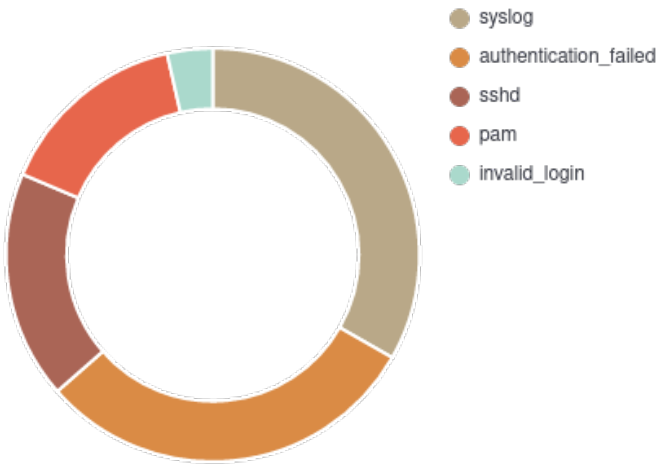
10

- Authentication success -

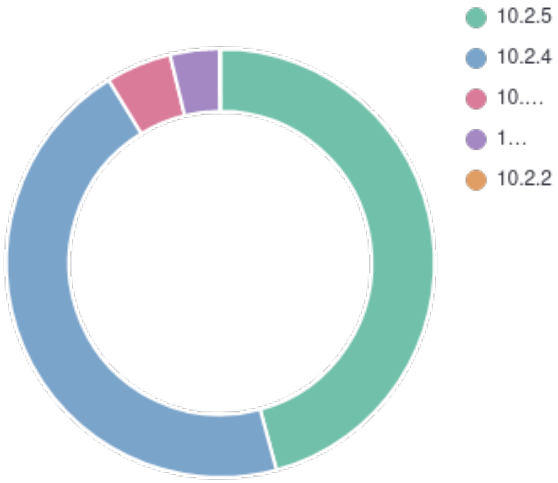
Top 5 alerts



Top 5 rule groups



Top 5 PCI DSS Requirements



Alerts summary

Rule ID	Description	Level	Count
5503	PAM: User login failed.	5	1538
5760	sshd: authentication failed.	5	1517
5710	sshd: Attempt to login using a non-existent user	5	413
5551	PAM: Multiple failed logins in a small period of time.	10	200
5763	sshd: brute force trying to get access to the system. Authentication failed.	10	101
2502	syslog: User missed the password more than one time	10	32
5758	Maximum authentication attempts exceeded.	8	21
5712	sshd: brute force trying to get access to the system. Non existent user.	10	11
5502	PAM: Login session closed.	3	8
5501	PAM: Login session opened.	3	7
5762	sshd: connection reset	4	6
550	Integrity checksum changed.	7	4
5740	sshd: connection reset by peer	4	4
2501	syslog: User authentication failure.	5	3
5402	Successful sudo to ROOT executed.	3	3
5715	sshd: authentication success.	3	3
11	-	-	2
510	Host-based anomaly detection event (rootcheck).	7	2
5405	Unauthorized user attempted to use sudo.	5	2
2961	User added to group sudo.	5	1
5403	First time user executed sudo.	4	1

Groups summary

Groups	Count
syslog	3871
authentication_failed	3524
sshd	2076
pam	1753
invalid_login	413
authentication_failures	312
access_control	35
authentication_success	10
ossec	6
sudo	6
syscheck	4
syscheck_entry_modified	4
syscheck_file	4
rootcheck	2
stats	2
yum	1