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	Oct 31, 2024 @ 02:57:54.000

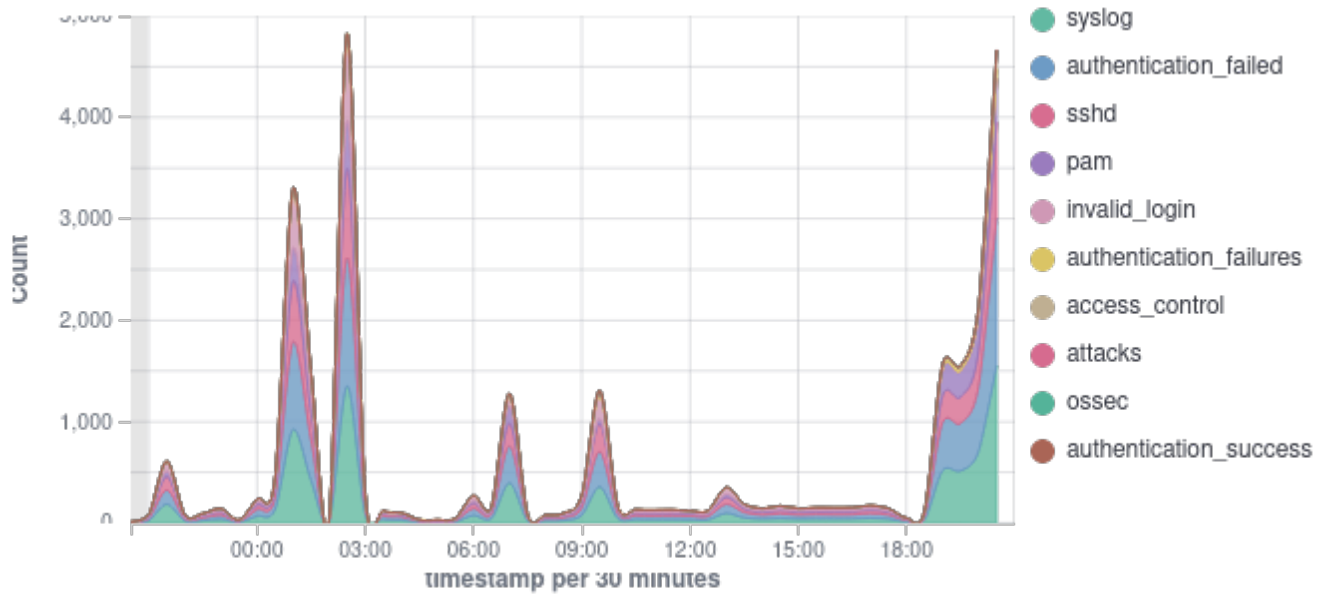
Group: default

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

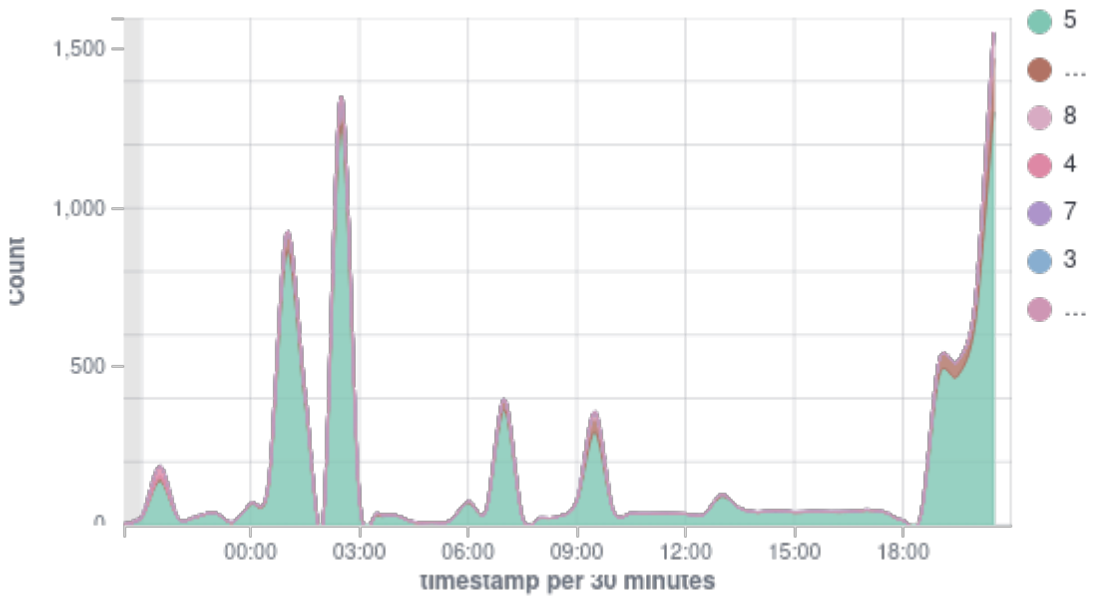
2024-10-29T20:57:53 to 2024-10-30T20:57:53

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

Top 10 Alert groups evolution



Alerts



8,507

- Total -

1

- Level 12 or above alerts -

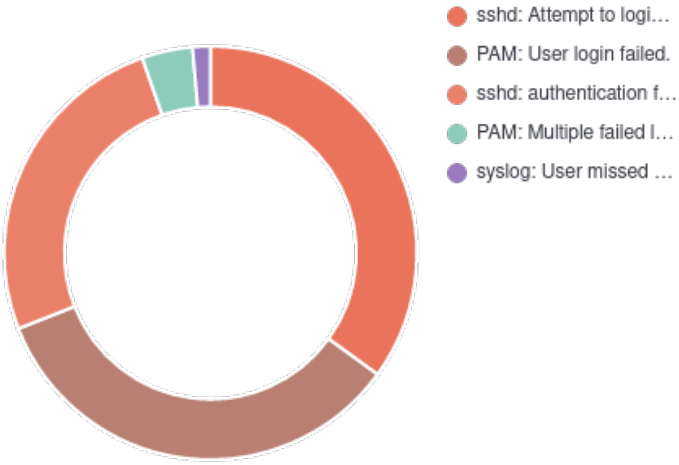
8,421

- Authentication failure -

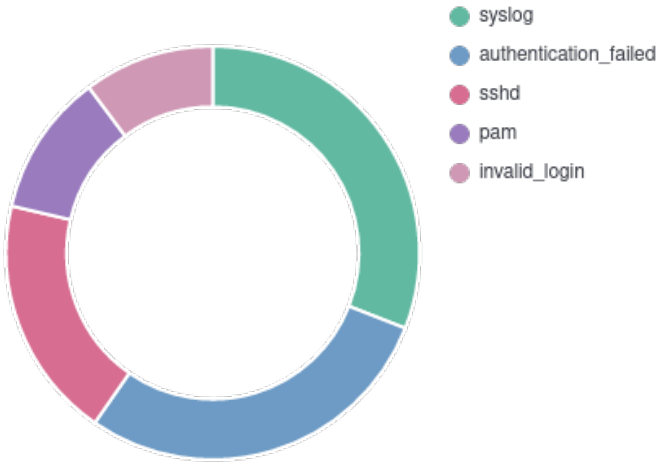
4

- Authentication success -

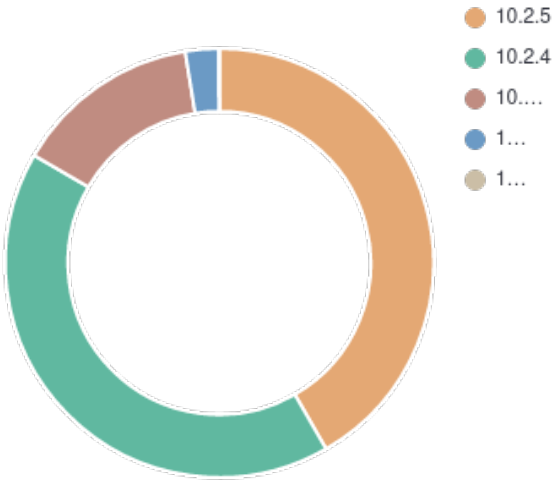
Top 5 alerts



Top 5 rule groups



Top 5 PCI DSS Requirements



Alerts summary

Rule ID	Description	Level	Count
5710	sshd: Attempt to login using a non-existent user	5	2808
5503	PAM: User login failed.	5	2733
5760	sshd: authentication failed.	5	2057
5551	PAM: Multiple failed logins in a small period of time.	10	320
2502	syslog: User missed the password more than one time	10	111
5758	Maximum authentication attempts exceeded.	8	99
5712	sshd: brute force trying to get access to the system. Non existent user.	10	93
5763	sshd: brute force trying to get access to the system. Authentication failed.	10	93
2501	syslog: User authentication failure.	5	90
5762	sshd: connection reset	4	47
40111	Multiple authentication failures.	10	22
5740	sshd: connection reset by peer	4	22
510	Host-based anomaly detection event (rootcheck).	7	4
550	Integrity checksum changed.	7	4
5501	PAM: Login session opened.	3	3
11	-	-	2
2961	User added to group sudo.	5	1
40112	Multiple authentication failures followed by a success.	12	1
5502	PAM: Login session closed.	3	1
5715	sshd: authentication success.	3	1

Groups summary

Groups	Count
syslog	8502
authentication_failed	7898
sshd	5220
pam	3057
invalid_login	2808
authentication_failures	528
access_control	201
attacks	23
ossec	8
authentication_success	4
rootcheck	4
syscheck	4
syscheck_entry_modified	4
syscheck_file	4
stats	2
yum	1