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

Threat hunting report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
001	kali	192.168.0.25	Wazuh v4.9.2	debian	Kali GNU/Linux 2024.3	Nov 18, 2024 @ 15:28:30.000	Nov 18, 2024 @ 17:56:37.000

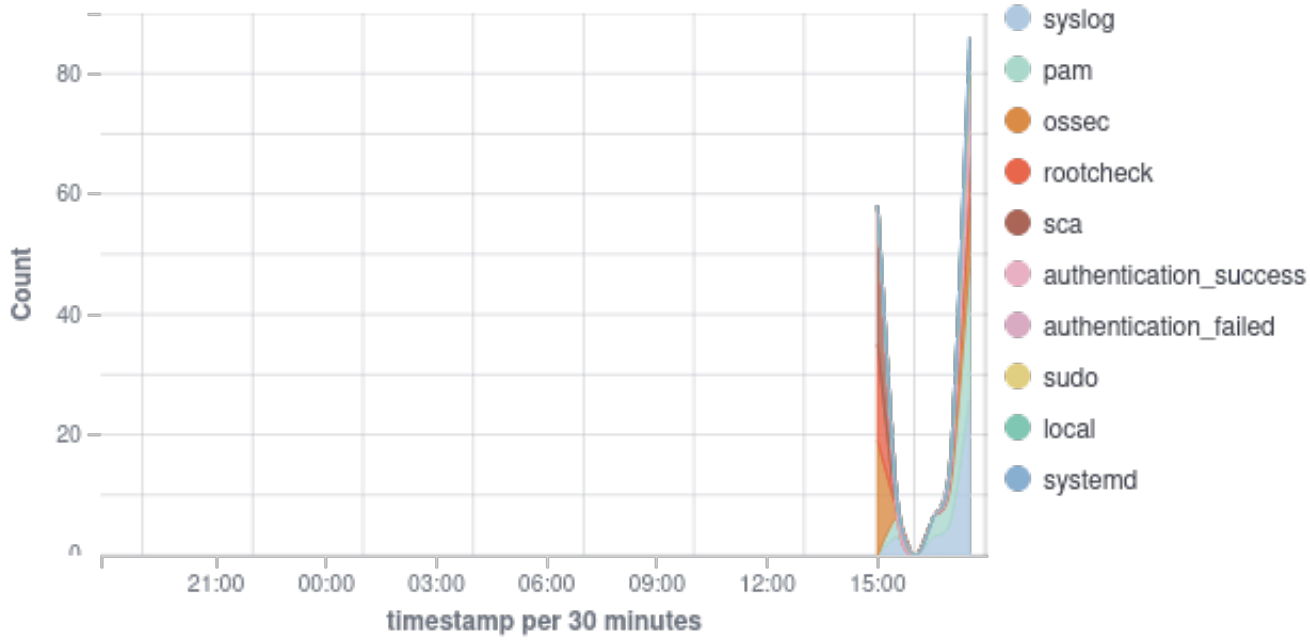
Group: default

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

2024-11-17T17:56:41 to 2024-11-18T17:56:41

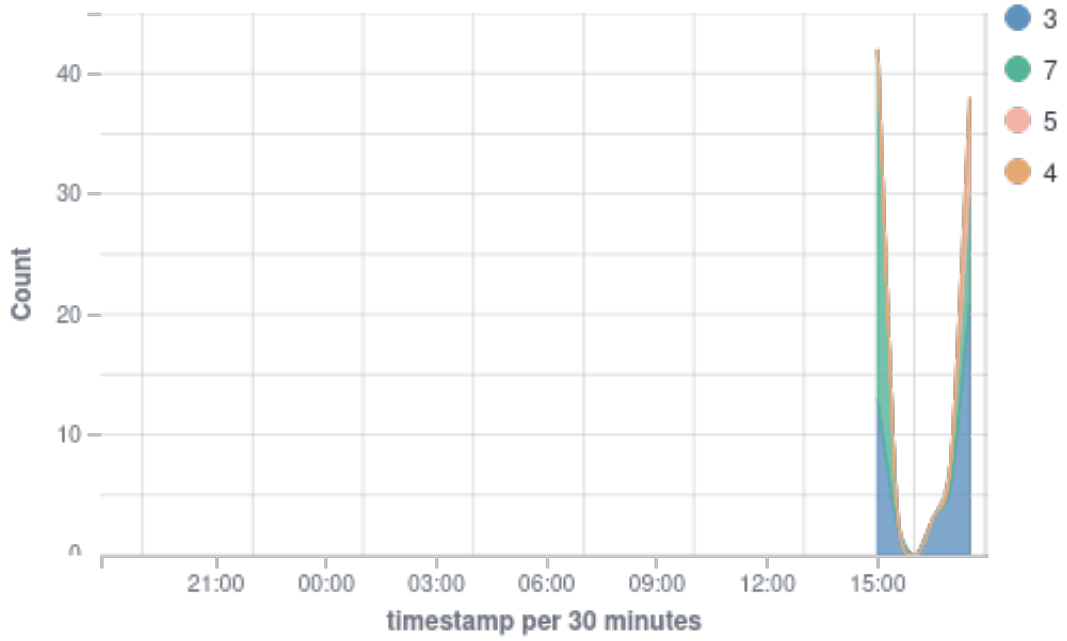
manager.name: debian AND agent.id: 001

Top 10 Alert groups evolution



Copyright © Wazuh, Inc.

Alerts



96
- Total -

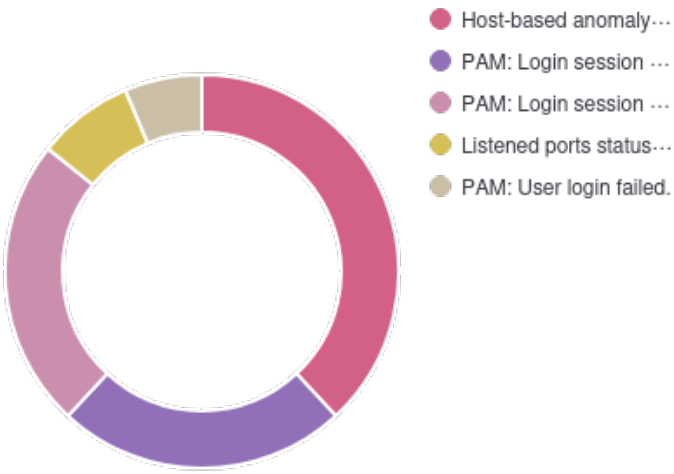
0
- Level 12 or above alerts -

4
- Authentication failure -

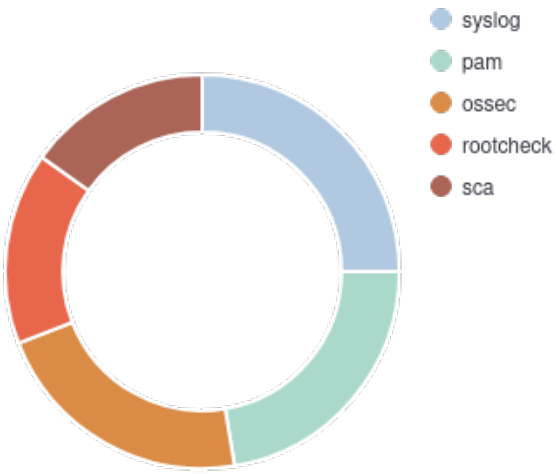
15
- Authentication success -

Copyright © Wazuh, Inc.

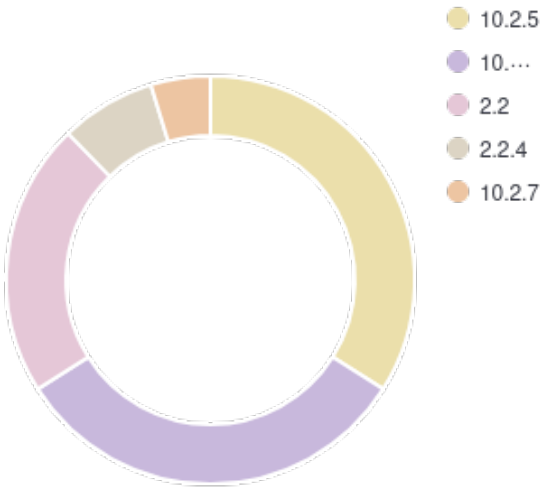
Top 5 alerts



Top 5 rule groups



Top 5 PCI DSS Requirements



Copyright © Wazuh, Inc.

Alerts summary

Rule ID	Description	Level	Count
510	Host-based anomaly detection event (rootcheck).	7	24
5501	PAM: Login session opened.	3	16
5502	PAM: Login session closed.	3	16
533	Listened ports status (netstat) changed (new port opened or closed).	7	5
5503	PAM: User login failed.	5	4
5402	Successful sudo to ROOT executed.	3	3
40704	Systemd: Service exited due to a failure.	5	2
503	Wazuh agent started.	3	2
19007	System audit for Unix based systems: Ensure auditd service is enabled	7	1
19007	System audit for Unix based systems: Ensure lockout for failed password attempts is configured	7	1
19007	System audit for Unix based systems: Ensure password expiration is 365 days or less	7	1
19007	System audit for Unix based systems: SSH Hardening: Empty passwords should not be allowed	7	1
19007	System audit for Unix based systems: SSH Hardening: Ensure SSH HostbasedAuthentication is disabled	7	1
19007	System audit for Unix based systems: SSH Hardening: Grace Time should be one minute or less.	7	1
19007	System audit for Unix based systems: SSH Hardening: No Public Key authentication	7	1
19007	System audit for Unix based systems: SSH Hardening: Password Authentication should be disabled	7	1
19007	System audit for Unix based systems: SSH Hardening: Port should not be 22	7	1
19007	System audit for Unix based systems: SSH Hardening: Protocol should be set to 2	7	1
19007	System audit for Unix based systems: SSH Hardening: Rhost or shost should not be used for authentication	7	1
19007	System audit for Unix based systems: SSH Hardening: Root account should not be able to log in	7	1
19007	System audit for Unix based systems: SSH Hardening: Wrong Maximum number of authentication attempts	7	1
19009	System audit for Unix based systems: Ensure password hashing algorithm is SHA-512	3	1
19009	System audit for Unix based systems: Ensure passwords are longer than 14 characters	3	1
19009	System audit for Unix based systems: Ensure passwords contain at least one digit	3	1
19009	System audit for Unix based systems: Ensure passwords contain at least one lowercase character	3	1
19009	System audit for Unix based systems: Ensure passwords contain at least one special character	3	1
19009	System audit for Unix based systems: Ensure passwords contain at least one uppercase character	3	1
19009	System audit for Unix based systems: Ensure retry option for passwords is less than 3	3	1
19008	System audit for Unix based systems: Ensure CUPS is not enabled	3	1
19008	System audit for Unix based systems: Ensure SELinux or AppArmor are installed	3	1
19008	System audit for Unix based systems: Ensure passwords in /etc/shadow are hashed with SHA-512 or SHA-256	3	1
1004	Syslogd exiting (logging stopped).	5	1
501	New wazuh agent connected.	3	1
506	Wazuh agent stopped.	3	1
5403	First time user executed sudo.	4	1

Copyright © Wazuh, Inc.

Groups summary

Groups	Count
syslog	41
pam	36
ossec	33
rootcheck	24
sca	23
authentication_success	16
authentication_failed	4
sudo	4
local	2
systemd	2
errors	1

Copyright © Wazuh, Inc.