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

Security events report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
001	kali-agent	172.30.251.234	Wazuh v4.7.4	ubantu	Kali GNU/Linux 2025.2	Jun 28, 2025 @ 13:10:24.000	Jun 28, 2025 @ 13:13:36.000

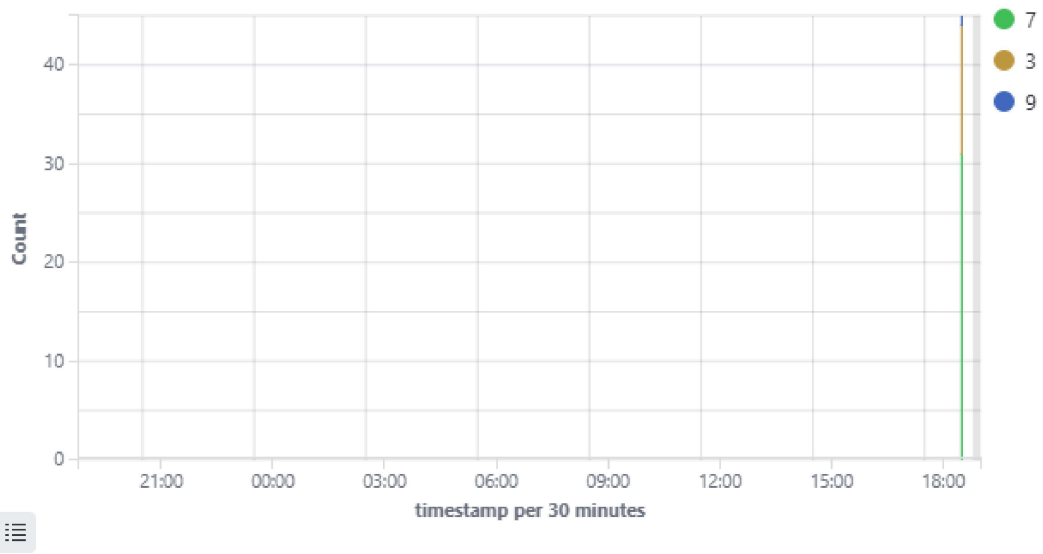
Group: default

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

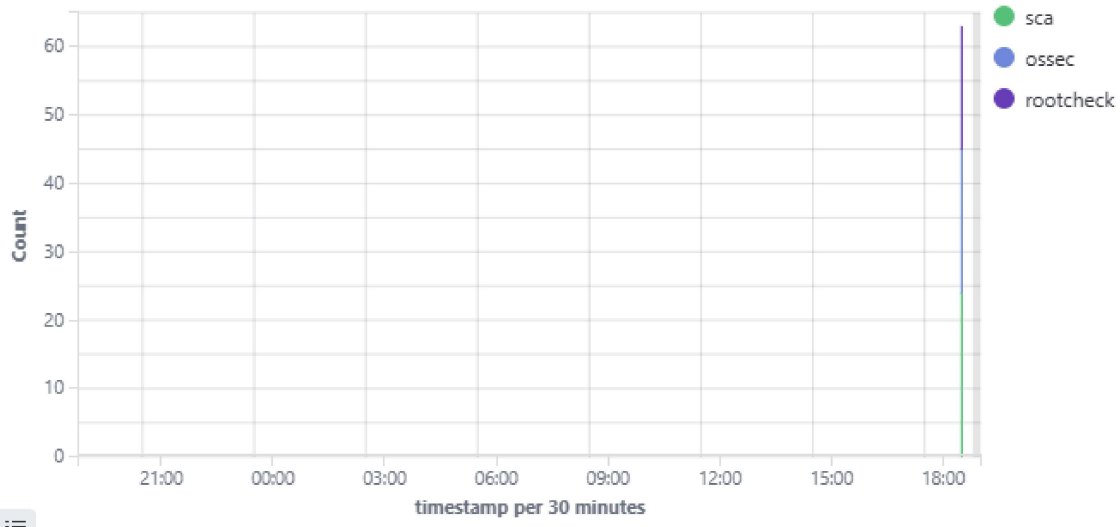
2025-06-27T18:48:18 to 2025-06-28T18:48:18

manager.name: ubantu AND agent.id: 001

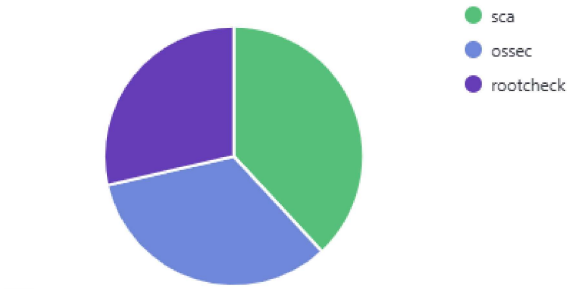
Alerts



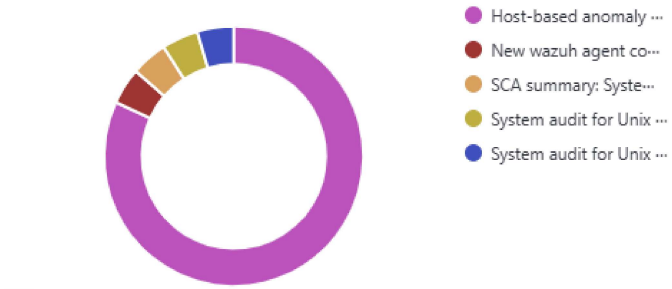
Alert groups evolution



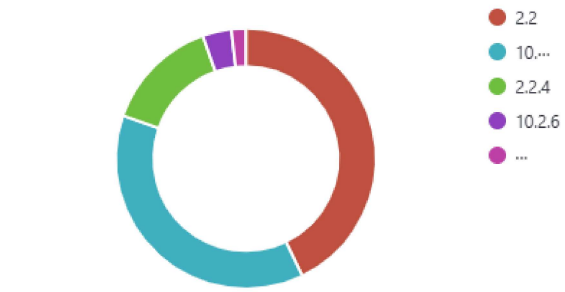
Top 5 rule groups



Top 5 alerts



Top 5 PCI DSS requirements



Alerts summary

Rule ID	Description	Level	Count
510	Host-based anomaly detection event (rootcheck).	7	18
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
19005	SCA summary: System audit for Unix based systems: Score less than 30% (18)	9	1
501	New wazuh agent connected.	3	1
503	Wazuh agent started.	3	1
506	Wazuh agent stopped.	3	1

Groups summary

Groups	Count
sca	24
ossec	21
rootcheck	18