wazuh.

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

Threat hunting report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
001	kali	192.168.84.135	Wazuh v4.12.0	siem-VMware-Virtual-Platform	Kali GNU/Linux 2025.3	Sep 9, 2025 @ 15:07:31.000	Oct 6, 2025 @ 19:03:25.000

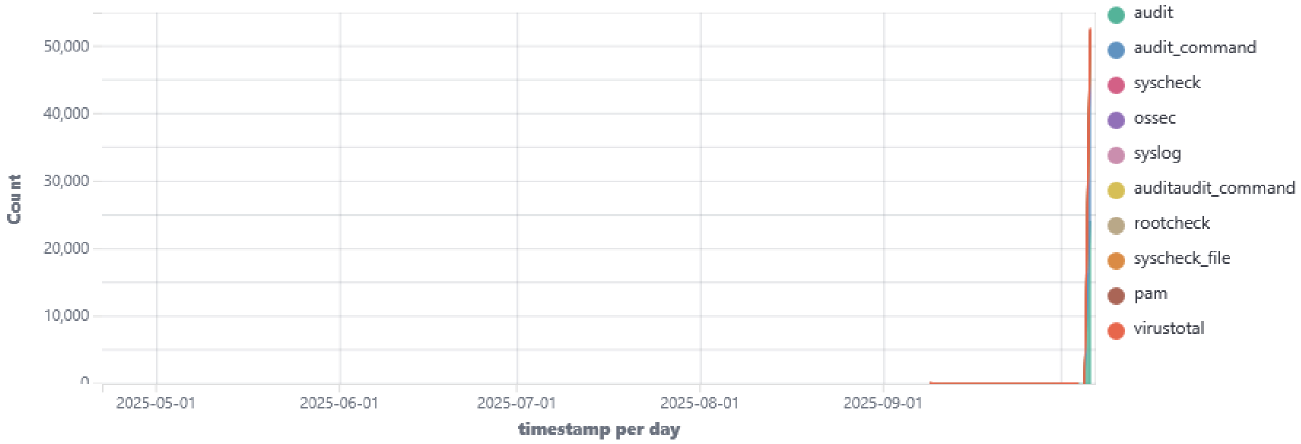
Group: default

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

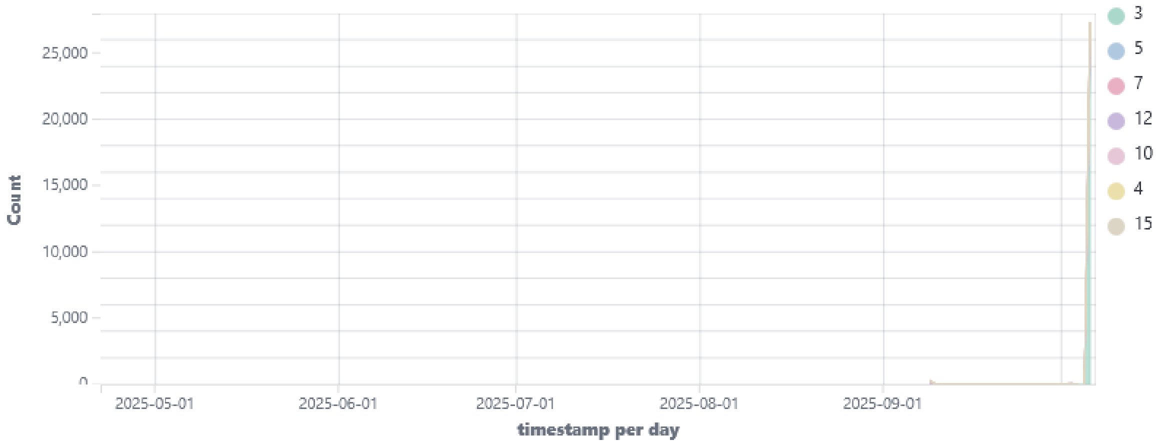
2025-04-21T19:03:29 to 2025-10-06T19:03:29

manager.name: siem-VMware-Virtual-Platform AND agent.id: 001

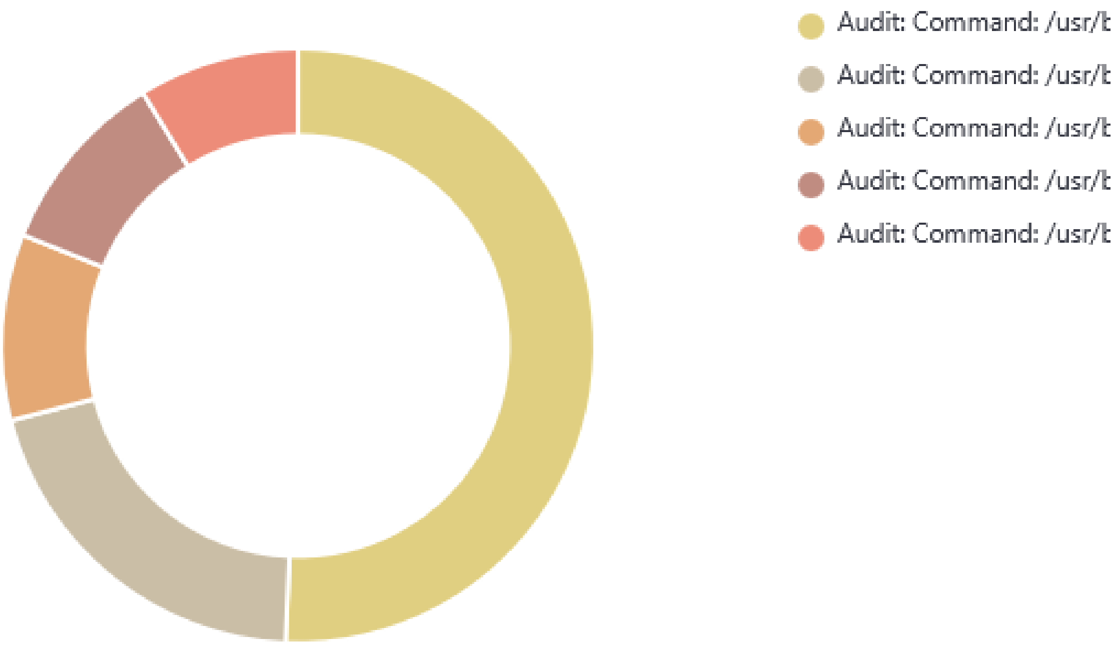
Top 10 Alert groups evolution



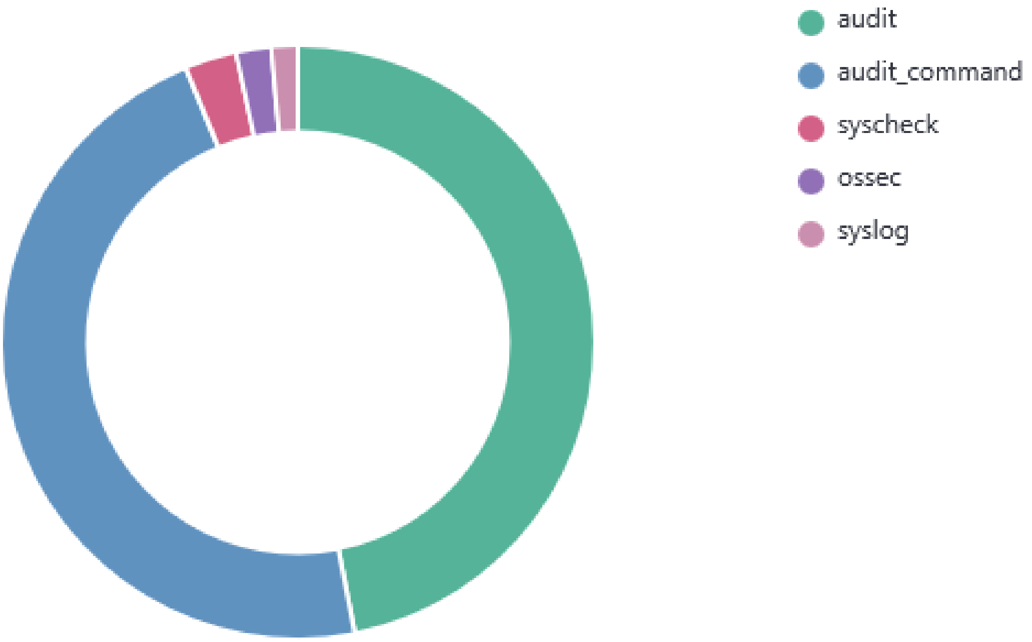
Alerts



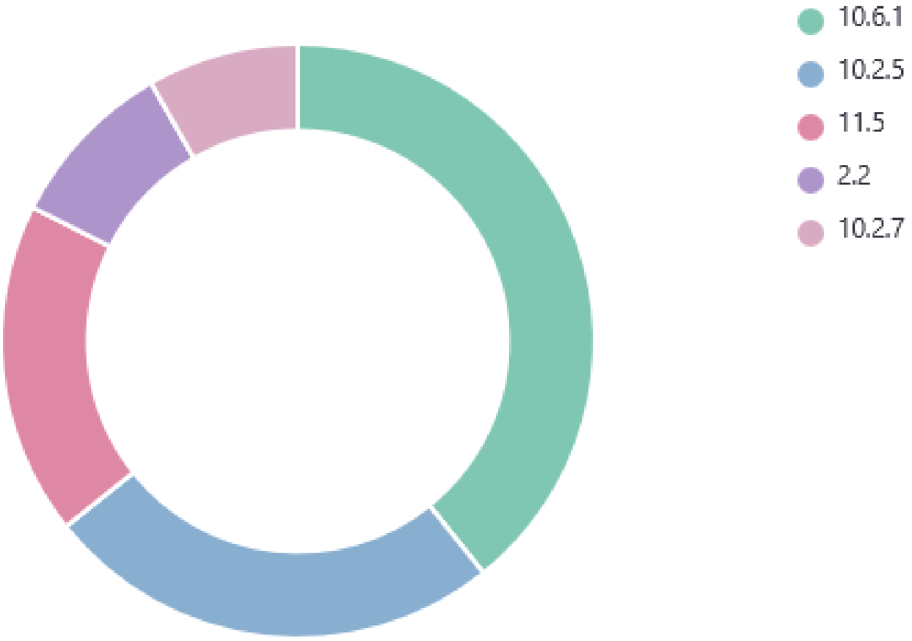
Top 5 alerts



Top 5 rule groups



Top 5 PCI DSS Requirements



28,030
- Total -

558
- Level 12 or above alerts -

11
- Authentication failure -

185
- Authentication success -

Copyright © Wazuh, Inc.

Alerts summary

Rule ID	Description	Level	Count
80792	Audit: Command: /usr/bin/gnome.	3	11015
80792	Audit: Command: /usr/bin/ip.	3	4408
80792	Audit: Command: /usr/bin/cut.	3	2204
80792	Audit: Command: /usr/bin/head.	3	2204
80792	Audit: Command: /usr/bin/dash.	3	1904
100300	File modified in /home directory.	5	931
510	Host-based anomaly detection event (rootcheck).	7	503
80792	Audit: Command: /usr/bin/x86_64.	3	426
100210	Audit: Highly Suspicious Command executed: /usr/bin/dash	12	426
80792	Audit: Command: /usr/bin/sed.	3	384
87103	VirusTotal: Alert - No records in VirusTotal database	3	281
80792	Audit: Command: /usr/bin/rm.	3	249
5501	PAM: Login session opened.	3	185
5502	PAM: Login session closed.	3	182
80792	Audit: Command: /usr/bin/dpkg.	3	159
5402	Successful sudo to ROOT executed.	3	148
553	File deleted.	7	143
100301	File added to /home directory.	5	135
80792	Audit: Command: /usr/bin/cat.	3	126
550	Integrity checksum changed.	7	116
554	File added to the system.	5	116
80792	Audit: Command: /usr/libexec/gcc/x86_64.	3	107
40704	Systemd: Service exited due to a failure.	5	84
2904	Dpkg (Debian Package) half configured.	7	81
80792	Audit: Command: /usr/bin/perl.	3	78
2902	New dpkg (Debian Package) installed.	7	73
100210	Audit: Highly Suspicious Command executed: /usr/bin/bash	12	70
80792	Audit: Command: /usr/bin/grep.	3	65
80792	Audit: Command: /usr/bin/basename.	3	52
2901	New dpkg (Debian Package) requested to install.	3	47
80792	Audit: Command: /usr/bin/m4.	3	46
80792	Audit: Command: /usr/sbin/unix_chkpwd.	3	44
80792	Audit: Command: /usr/bin/make.	3	34
80792	Audit: Command: /usr/lib/apt/methods/http.	3	32
80792	Audit: Command: /usr/bin/test.	3	29
100210	Audit: Highly Suspicious Command executed: /usr/bin/sudo	12	29
80792	Audit: Command: /usr/local/bin/yara.	3	28
100210	Audit: Highly Suspicious Command executed: /usr/bin/nc	12	7
100210	Audit: Highly Suspicious Command executed: /usr/bin/chmod	12	4

Rule ID	Description	Level	Count
87104	VirusTotal: Alert - /home/kali/.local/share/nautilus/tags/meta.db-shm - No positives found	3	4
87104	VirusTotal: Alert - /home/kali/.local/share/nautilus/tags/meta.db-wal - No positives found	3	4
100210	Audit: Highly Suspicious Command executed: /usr/bin/su	12	2
87104	VirusTotal: Alert - /home/kali/.cache/mozilla/firefox/cs2lwm8z.default-esr/.startup-incomplete - No positives found	3	2
87104	VirusTotal: Alert - /home/kali/.cache/mozilla/firefox/cs2lwm8z.default-esr/cache2/ce_T151c2VyQ29udGV4dElkPTUs - No positives found	3	2
87104	VirusTotal: Alert - /home/kali/.mozilla/firefox/cs2lwm8z.default-esr/lock - No positives found	3	2
87104	VirusTotal: Alert - /home/kali/Desktop/Diamorphine/.git/hooks/push-to-checkout.sample - No positives found	3	2
87104	VirusTotal: Alert - /home/kali/Desktop/Diamorphine/.git/hooks/update.sample - No positives found	3	2
87104	VirusTotal: Alert - /home/kali/malware/3omda2.txt - No positives found	3	2
100210	Audit: Highly Suspicious Command executed: /usr/bin/curl	12	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Disable USB Storage.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure /etc/hosts.deny is configured.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure AIDE is installed.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure Avahi Server is not enabled.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DCCP is disabled.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure ICMP redirects are not accepted.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 default deny firewall policy.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 loopback traffic is configured.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 router advertisements are not accepted.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure LDAP client is not installed.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure RDS is disabled.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure Reverse Path Filtering is enabled.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SCTP is disabled.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SELinux is not disabled in bootloader configuration.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH AllowTcpForwarding is disabled.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH Idle Timeout Interval is configured.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH LoginGraceTime is set to one minute or less.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxAuthTries is set to 4 or less.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxSessions is set to 4 or less.	7	1
19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxStartups is configured.	7	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Disable Automounting.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure /tmp is configured.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure CUPS is not enabled.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DHCP Server is not enabled.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DNS Server is not enabled.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure FTP Server is not enabled.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure GDM login banner is configured.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Proxy Server is not enabled.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP server is not enabled.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IMAP and POP3 server is not enabled.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IP forwarding is disabled.	3	1

Rule ID	Description	Level	Count
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure LDAP server is not enabled.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure NFS and RPC are not enabled.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure NIS Client is not installed.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure NIS Server is not enabled.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SELinux or AppArmor are installed.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SETroubleshoot is not installed.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SNMP Server is not enabled.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH HostbasedAuthentication is disabled.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH IgnoreRhosts is enabled.	3	1
87104	VirusTotal: Alert - /home/kali/.cache/mesa_shader_cache_db/marker - No positives found	3	1
87104	VirusTotal: Alert - /home/kali/.cache/mozilla/firefox/cs2lwm8z.default-esr/activity-stream.weather_feed.json - No positives found	3	1
87104	VirusTotal: Alert - /home/kali/.cache/mozilla/firefox/cs2lwm8z.default-esr/cache2/ce_T151c2VyQ29udGV4dElkPTUsYSw= - No positives found	3	1
87104	VirusTotal: Alert - /home/kali/.cache/mozilla/firefox/cs2lwm8z.default-esr/safebrowsing/ads-track-digest256.vlpset - No positives found	3	1
87104	VirusTotal: Alert - /home/kali/.cache/mozilla/firefox/cs2lwm8z.default-esr/safebrowsing/social-tracking-protection-twitter-digest256.vlpset - No positives found	3	1
87104	VirusTotal: Alert - /home/kali/.cache/tracker3/files/http%3A%2F%2Ftracker.api.gnome.org%2Fontology%2Fv3%2Ftracker%23Pictures.db-shm - No positives found	3	1
87104	VirusTotal: Alert - /home/kali/.cache/tracker3/files/http%3A%2F%2Ftracker.api.gnome.org%2Fontology%2Fv3%2Ftracker%23Pictures.db-wal - No positives found	3	1
87104	VirusTotal: Alert - /home/kali/.cache/tracker3/files/http%3A%2F%2Ftracker.api.gnome.org%2Fontology%2Fv3%2Ftracker%23Software.db-shm - No positives found	3	1
87104	VirusTotal: Alert - /home/kali/.cache/tracker3/files/http%3A%2F%2Ftracker.api.gnome.org%2Fontology%2Fv3%2Ftracker%23Software.db-wal - No positives found	3	1
87104	VirusTotal: Alert - /home/kali/.mozilla/firefox/cs2lwm8z.default-esr/.parentlock - No positives found	3	1

Groups summary

Groups	Count
audit	24066
audit_command	24047
syscheck	1447
ossec	985
syslog	741
auditaudit_command	539
rootcheck	503
syscheck_file	375
pam	372
virustotal	333
dpkg	201
sca	196
authentication_success	185
config_changed	154
sudo	150
syscheck_entry_deleted	143
syscheck_entry_added	116
syscheck_entry_modified	116
local	84
systemd	84
active_response	14
errors	12
audit_anom	11
authentication_failed	11
ids	9
suricata	9
audit_configuration	8
service_availability	6
attack	5
invalid_login	4
sshd	4
accesslog	3
web	3
access_control	2
process_monitor	2
sql_injection	1