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

# Threat hunting report

Warning. Agent is disconnected

| 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 3, 2025 @ 17:50:49.000 |

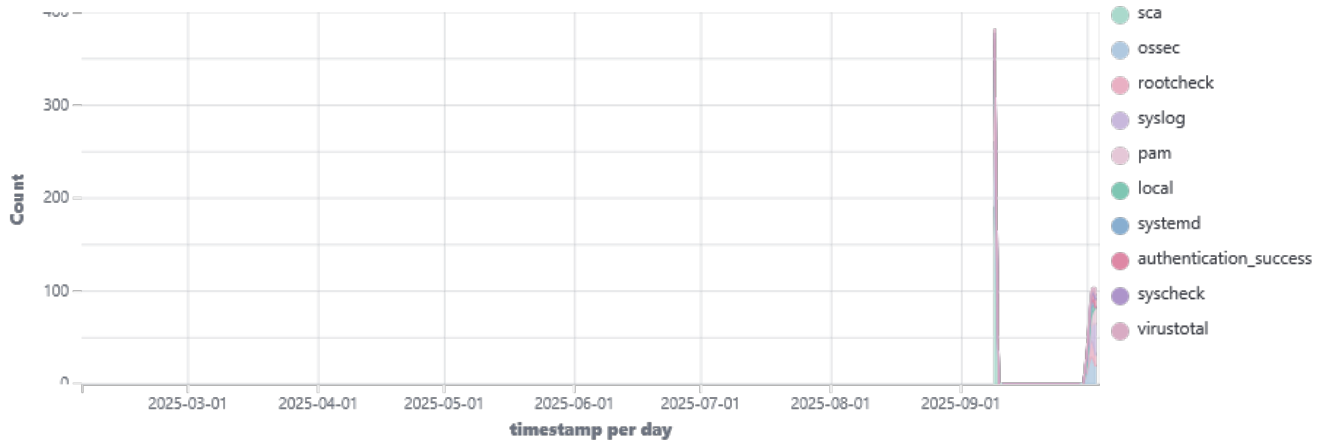
Group: default

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

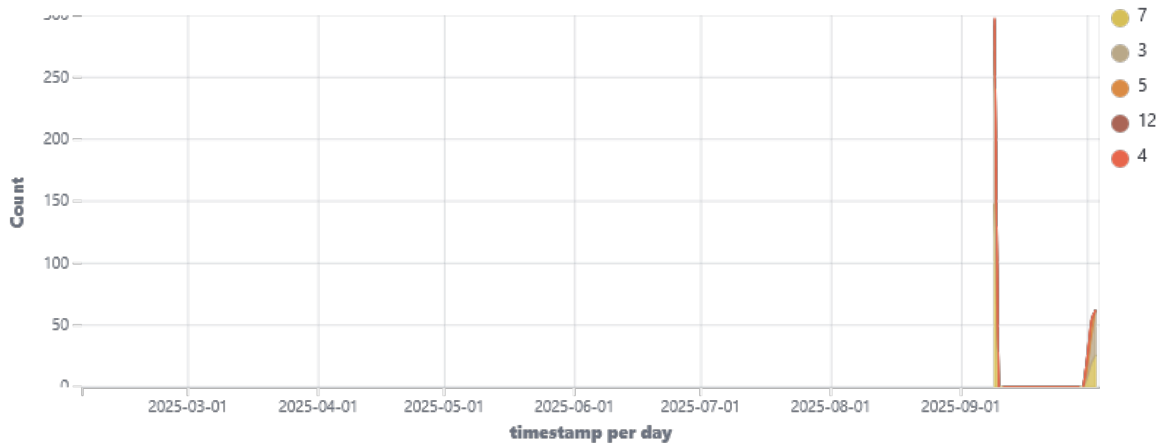
2025-02-03T17:55:34 to 2025-10-03T17:47:03

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

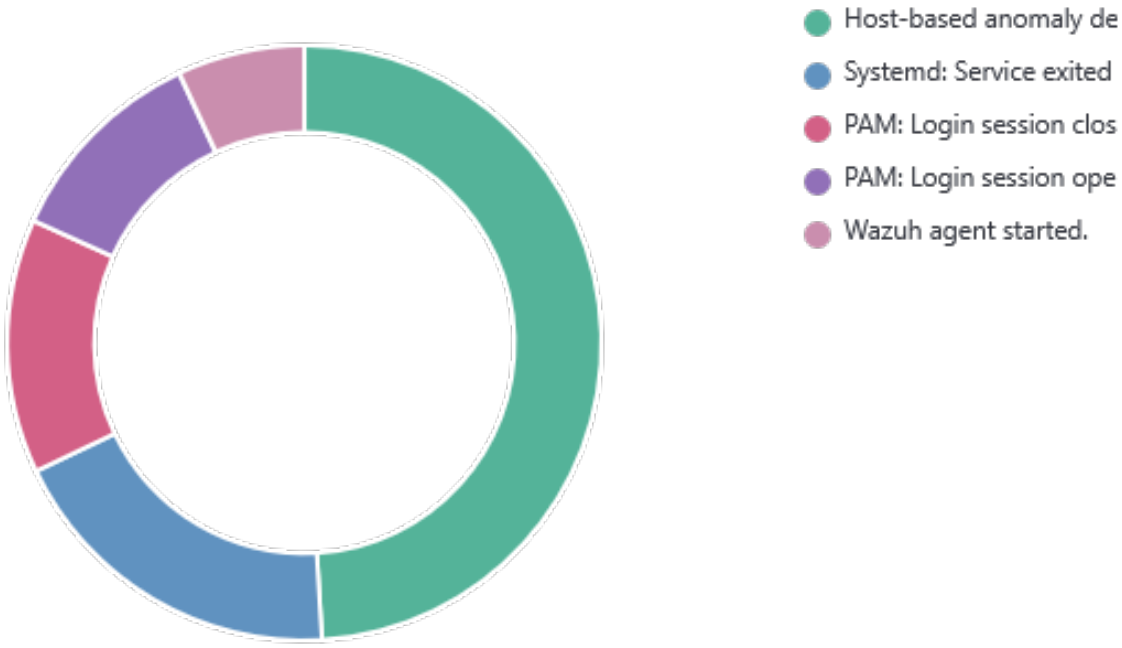
## Top 10 Alert groups evolution



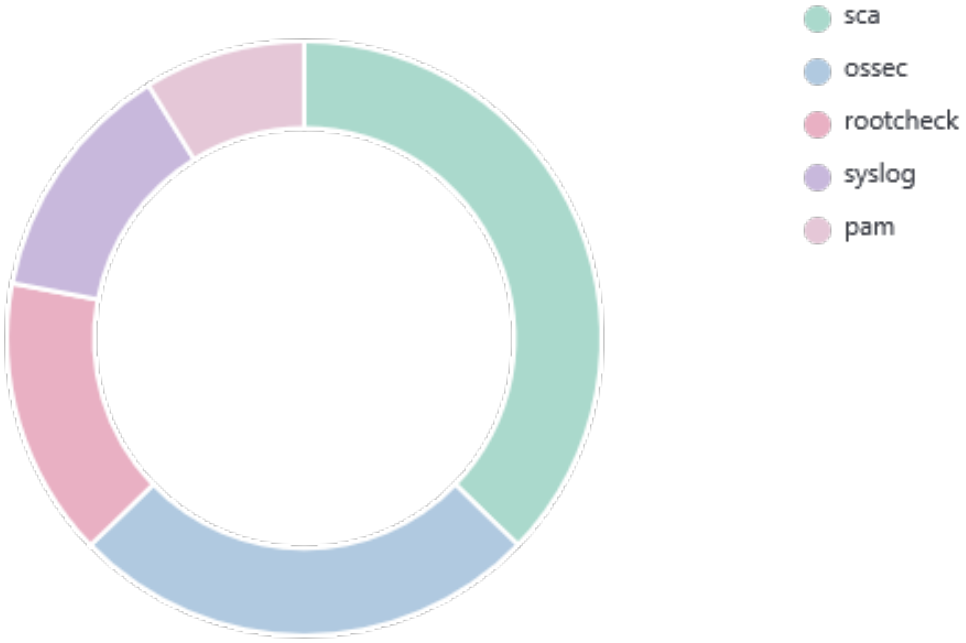
## Alerts



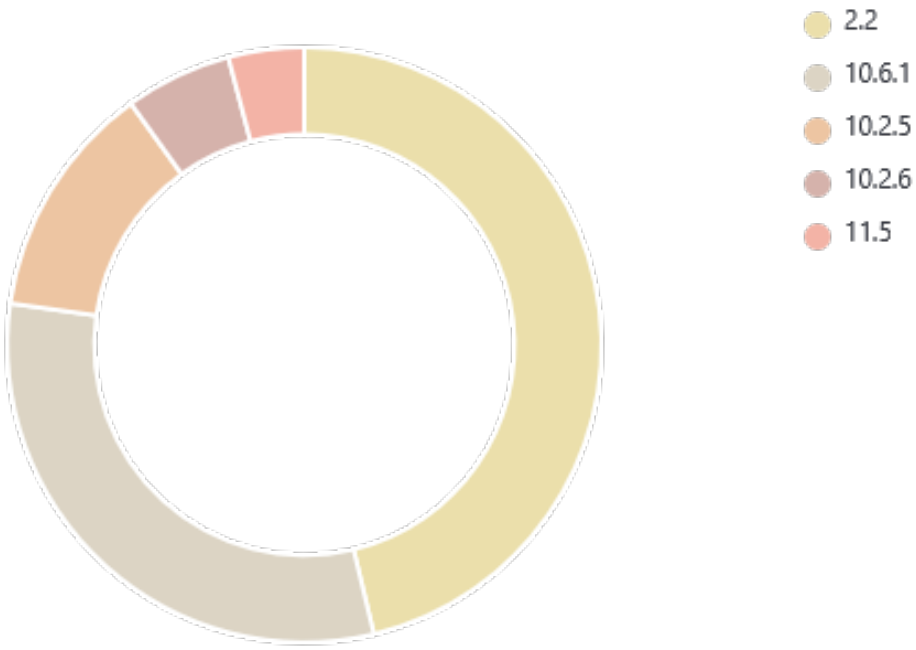

## Top 5 alerts



## Top 5 rule groups




## Top 5 PCI DSS Requirements



**438**
- Total -

**8**
- Level 12 or above alerts -

**2**
- Authentication failure -

**20**
- Authentication success -

## Alerts summary

| Rule ID | Description | Level | Count |
|---|---|---|---|
| 510 | Host-based anomaly detection event (rootcheck). | 7 | 78 |
| 40704 | Systemd: Service exited due to a failure. | 5 | 30 |
| 5502 | PAM: Login session closed. | 3 | 23 |
| 5501 | PAM: Login session opened. | 3 | 20 |
| 503 | Wazuh agent started. | 3 | 12 |
| 506 | Wazuh agent stopped. | 3 | 12 |
| 5402 | Successful sudo to ROOT executed. | 3 | 8 |
| 553 | File deleted. | 7 | 8 |
| 657 | Active response: active-response/bin/remove-threat.sh - add | 3 | 8 |
| 554 | File added to the system. | 5 | 7 |
| 87105 | VirusTotal: Alert - /home/kali/malware/ecir - 66 engines detected this file | 12 | 6 |
| 87103 | VirusTotal: Alert - No records in VirusTotal database | 3 | 6 |
| 2902 | New dpkg (Debian Package) installed. | 7 | 4 |
| 2904 | Dpkg (Debian Package) half configured. | 7 | 4 |
| 533 | Listened ports status (netstat) changed (new port opened or closed). | 7 | 4 |
| 1004 | Syslogd exiting (logging stopped). | 5 | 3 |
| 87105 | VirusTotal: Alert - /home/kali/malware/ecir - 65 engines detected this file | 12 | 2 |
| 100201 | File added to /home/kali/malware | 7 | 2 |
| 2901 | New dpkg (Debian Package) requested to install. | 3 | 2 |
| 5403 | First time user executed sudo. | 4 | 2 |
| 87104 | VirusTotal: Alert - /home/kali/malware/3omda2.txt - No positives found | 3 | 2 |
| 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 |

| Rule ID | Description | Level | Count |
|---|---|---|---|
| 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 |
| 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 |
| 19009 | CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure AppArmor is not disabled in bootloader configuration. | 3 | 1 |
| 19009 | CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SELinux policy is configured. | 3 | 1 |
| 19009 | CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure password creation requirements are configured. | 3 | 1 |
| 19009 | CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure password hashing algorithm is SHA-512. | 3 | 1 |
| 19009 | CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure password reuse is limited. | 3 | 1 |
| 19009 | CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure the SELinux state is enforcing. | 3 | 1 |
| 19009 | CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure the audit configuration is immutable. | 3 | 1 |
| 19004 | SCA summary: CIS Distribution Independent Linux Benchmark v2.0.0.: Score less than 50% (45) | 7 | 1 |
| 501 | New wazuh agent connected. | 3 | 1 |
| 5503 | PAM: User login failed. | 5 | 1 |
| 5557 | unix_chkpwd: Password check failed. | 5 | 1 |
| 591 | Log file rotated. | 3 | 1 |

## Groups summary

| Groups | Count |
|---|---|
| sca | 191 |
| ossec | 131 |
| rootcheck | 78 |
| syslog | 68 |
| pam | 45 |
| local | 30 |
| systemd | 30 |
| authentication_success | 20 |
| syscheck | 17 |
| virustotal | 16 |
| syscheck_file | 15 |
| dpkg | 10 |
| sudo | 10 |
| active_response | 8 |
| config_changed | 8 |
| syscheck_entry_deleted | 8 |
| syscheck_entry_added | 7 |
| errors | 3 |
| authentication_failed | 2 |