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

Threat hunting report

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

2025-10-20T03:56:51 to 2025-10-21T03:56:51

manager.name: Wazuh

1,383

- Total -

1

- Level 12 or above alerts -

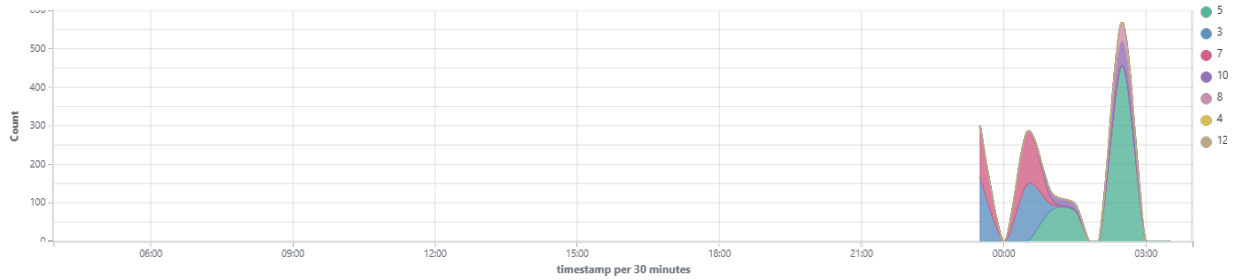
760

- Authentication failure -

9

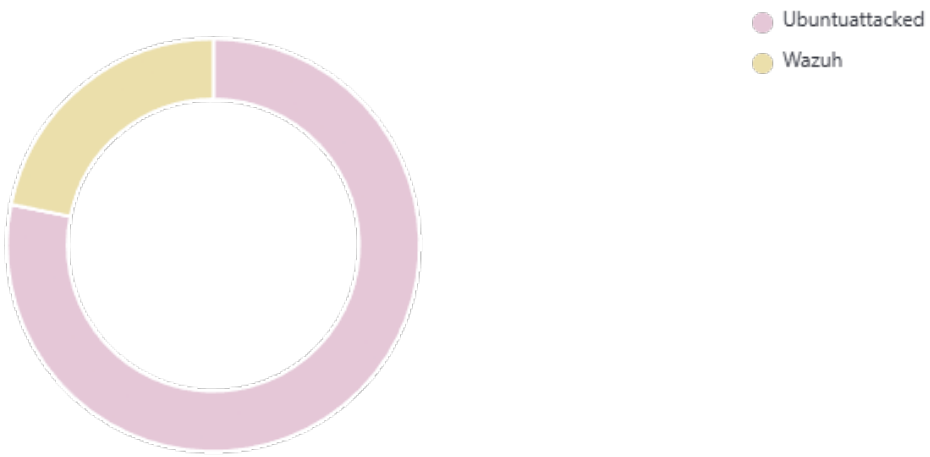
- Authentication success -

Top 10 Alert level evolution



Top 10 MITRE ATT&CKS

Top 5 agents



Alerts evolution - Top 5 agents

Alerts summary

Rule ID	Description	Level	Count
5710	sshd: Attempt to login using a non-existent user	5	544
2502	syslog: User missed the password more than one time	10	80
5503	PAM: User login failed.	5	72
5758	Maximum authentication attempts exceeded.	8	50
2902	New dpkg (Debian Package) installed.	7	10
2904	Dpkg (Debian Package) half configured.	7	10
5502	PAM: Login session closed.	3	10
5501	PAM: Login session opened.	3	9
2901	New dpkg (Debian Package) requested to install.	3	8
5551	PAM: Multiple failed logins in a small period of time.	10	8
5712	sshd: brute force trying to get access to the system. Non existent user.	10	6
502	Wazuh server started.	3	3
5403	First time user executed sudo.	4	3
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure /tmp is a separate partition.	7	2
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure AIDE is installed.	7	2
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure AppArmor is enabled in the bootloader configuration.	7	2
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure AppArmor is installed.	7	2
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure Automatic Error Reporting is not enabled.	7	2
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure GDM is removed.	7	2
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure a nftables table exists.	7	2
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure access to all logfiles has been configured.	7	2
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure access to bootloader config is configured.	7	2
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure access to the su command is restricted.	7	2
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure all AppArmor Profiles are enforcing.	7	2
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure all AppArmor Profiles are in enforce or complain mode.	7	2
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure at is restricted to authorized users.	7	2
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure audit tools group owner is configured.	7	2
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure audit tools owner is configured.	7	2
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure audit_backlog_limit is sufficient.	7	2
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure auditd packages are installed.	7	2
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure auditd service is enabled and active.	7	2
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure auditing for processes that start prior to auditd is enabled.	7	2
19007	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure bootloader password is set.	7	2
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure /dev/shm is a separate partition.	3	2
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure /etc/shadow password fields are not empty.	3	2
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure NIS Client is not installed.	3	2
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure X window server services are not in use.	3	2
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure XDMCP is not enabled.	3	2

Rule ID	Description	Level	Count
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure a single firewall configuration utility is in use.	3	2
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure access to /etc/issue is configured.	3	2
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure access to /etc/issue.net is configured.	3	2
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure access to /etc/motd is configured.	3	2
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure accounts in /etc/passwd use shadowed passwords.	3	2
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure address space layout randomization is enabled.	3	2
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure all groups in /etc/passwd exist in /etc/group.	3	2
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure audit configuration files group owner is configured.	3	2
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure audit configuration files mode is configured.	3	2
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure audit configuration files owner is configured.	3	2
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure audit tools mode is configured.	3	2
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure autofs services are not in use.	3	2
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure avahi daemon services are not in use.	3	2
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure bluetooth services are not in use.	3	2
19008	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure bogus icmp responses are ignored.	3	2
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure GDM automatic mounting of removable media is disabled.	3	2
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure GDM autorun-never is enabled.	3	2
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure GDM autorun-never is not overridden.	3	2
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure GDM disable-user-list option is enabled.	3	2
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure GDM disabling automatic mounting of removable media is not overridden.	3	2
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure GDM login banner is configured.	3	2
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure GDM screen locks cannot be overridden.	3	2
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure actions as another user are always logged.	3	2
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure audit log files group owner is configured.	3	2
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure audit log storage size is configured.	3	2
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure audit logs are not automatically deleted.	3	2
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure changes to system administration scope (sudoers) is collected.	3	2
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure cryptographic mechanisms are used to protect the integrity of audit tools.	3	2
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure default user umask is configured.	3	2
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure discretionary access control permission modification events are collected.	3	2
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure events that modify date and time information are collected.	3	2
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure events that modify the sudo log file are collected.	3	2
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure events that modify the system's Mandatory Access Controls are collected.	3	2
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure events that modify the system's network environment are collected.	3	2
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure events that modify user/group information are collected.	3	2
19004	SCA summary: CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Score less than 50% (42)	7	2
5402	Successful sudo to ROOT executed.	3	2

Rule ID	Description	Level	Count
19004	SCA summary: CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Score less than 50% (43)	7	1
40101	System user successfully logged to the system.	12	1
501	New wazuh agent connected.	3	1
503	Wazuh agent started.	3	1
506	Wazuh agent stopped.	3	1
5553	PAM misconfiguration.	4	1
5901	New group added to the system.	8	1
5902	New user added to the system.	8	1