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

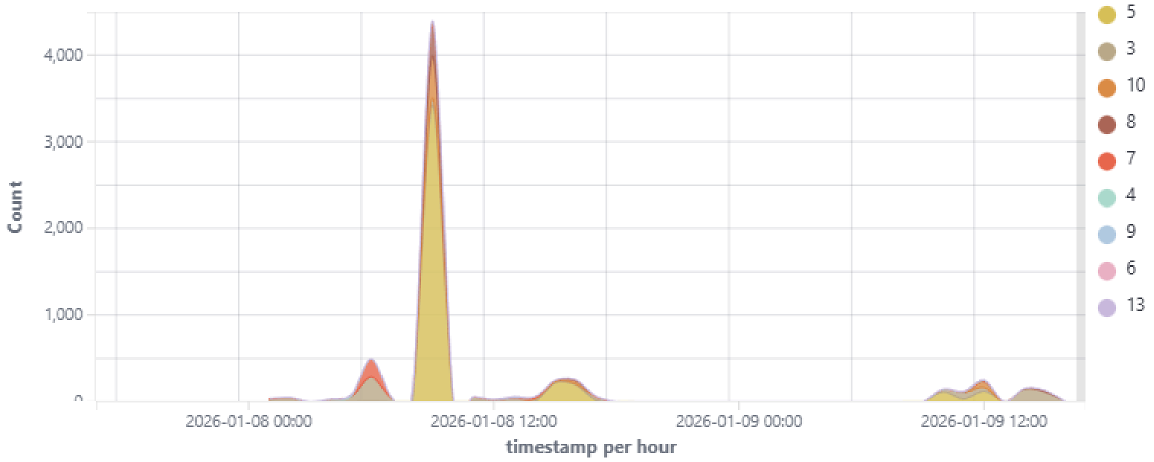
Threat hunting report

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

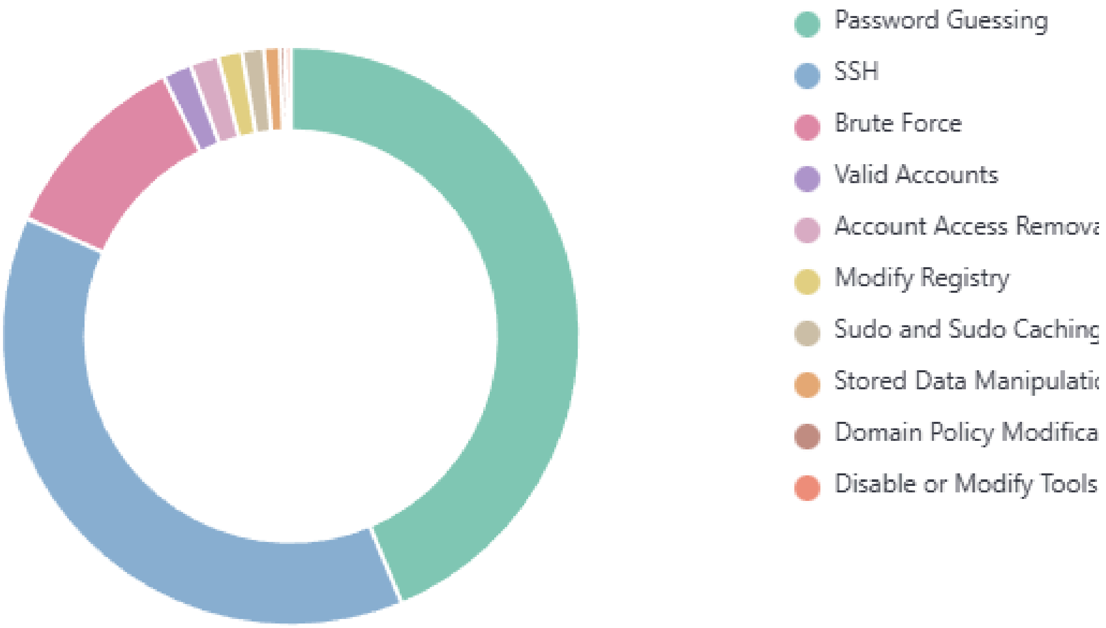
2026-01-07T16:31:41 to 2026-01-09T16:31:41

manager.name: wazuh-server

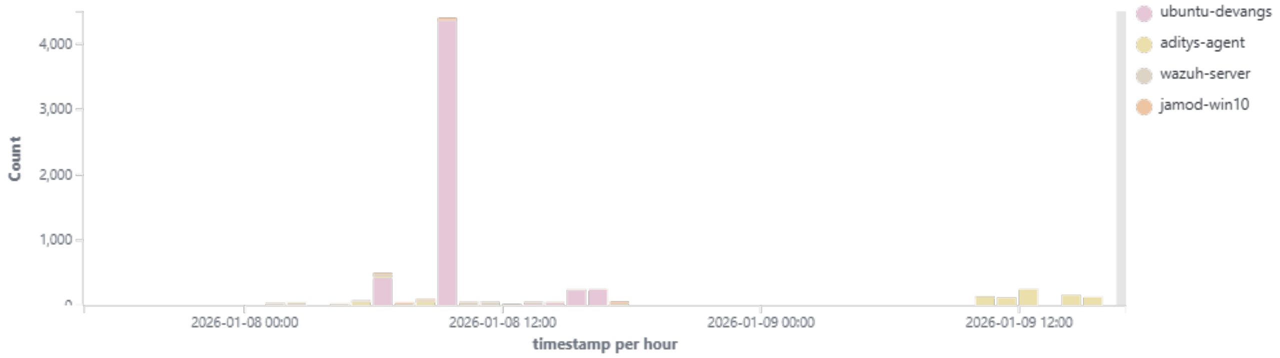
Top 10 Alert level evolution



Top 10 MITRE ATT&CKS



Alerts evolution - Top 5 agents



6,845

- Total -

1

- Level 12 or above alerts -

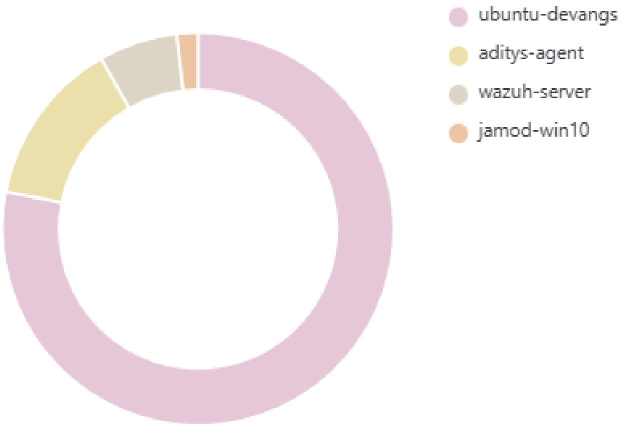
4,884

- Authentication failure -

138

- Authentication success -

Top 5 agents



Alerts summary

Rule ID	Description	Level	Count
5710	sshd: Attempt to login using a non-existent user	5	1936
5760	sshd: authentication failed.	5	1224
5503	PAM: User login failed.	5	477
2502	syslog: User missed the password more than one time	10	410
5758	Maximum authentication attempts exceeded.	8	374
67027	A process was created.	3	253
2501	syslog: User authentication failure.	5	193
60122	Logon Failure - Unknown user or bad password	5	131
5501	PAM: Login session opened.	3	125
5502	PAM: Login session closed.	3	125
60642	Software protection service scheduled successfully.	3	121
5402	Successful sudo to ROOT executed.	3	91
80730	Auditd: SELinux permission check.	3	77
5551	PAM: Multiple failed logins in a small period of time.	10	64
533	Listened ports status (netstat) changed (new port opened or closed).	7	52
40111	Multiple authentication failures.	10	48
594	Registry Key Integrity Checksum Changed	5	38
61104	Service startup type was changed	3	38
750	Registry Value Integrity Checksum Changed	5	37
19009	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure sudo is installed.	3	4
19007	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure /tmp is a separate partition.	7	2
19007	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure AIDE is installed.	7	2
19007	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure AppArmor is enabled in the bootloader configuration.	7	2
19007	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure Avahi Server is not installed.	7	2
19007	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure CUPS is not installed.	7	2
19007	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure GNOME Display Manager is removed.	7	2
19007	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure X Window System is not installed.	7	2
19007	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure access to the su command is restricted.	7	2
19007	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure actions as another user are always logged.	7	2
19007	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure all AppArmor Profiles are enforcing.	7	2
19007	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure at is	7	2

Rule ID	Description	Level	Count
	restricted to authorized users.		
19007	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure audit log storage size is configured.	7	2
19007	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure audit logs are not automatically deleted.	7	2
19007	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure audit_backlog_limit is sufficient.	7	2
19007	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure auditd is installed.	7	2
19007	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure auditd service is enabled and active.	7	2
19007	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure auditing for processes that start prior to auditd is enabled.	7	2
19007	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure bluetooth is disabled.	7	2
19007	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure bootloader password is set.	7	2
19007	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure changes to system administration scope (sudoers) is collected.	7	2
19008	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Disable Automounting.	3	2
19008	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure /etc/shadow password fields are not empty.	3	2
19008	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure AppArmor is installed.	3	2
19008	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure Automatic Error Reporting is not enabled.	3	2
19008	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure DHCP Server is not installed.	3	2
19008	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure DNS Server is not installed.	3	2
19008	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure FTP Server is not installed.	3	2
19008	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure HTTP Proxy Server is not installed.	3	2
19008	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure HTTP server is not installed.	3	2
19008	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure IMAP and POP3 server are not installed.	3	2
19008	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure IPv6 status is identified.	3	2
19008	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure LDAP client is not installed.	3	2
19008	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure LDAP server is not installed.	3	2
19008	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure NFS is not installed.	3	2
19008	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure NIS Client is not installed.	3	2

Rule ID	Description	Level	Count
19008	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure NIS Server is not installed.	3	2
19008	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure RPC is not installed.	3	2
19008	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure SNMP Server is not installed.	3	2
19008	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure Samba is not installed.	3	2
19008	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure XDCMP is not enabled.	3	2
19009	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure SSH AllowTcpForwarding is disabled.	3	2
19009	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure SSH HostbasedAuthentication is disabled.	3	2
19009	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure SSH Idle Timeout Interval is configured.	3	2
19009	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure SSH IgnoreRhosts is enabled.	3	2
19009	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure SSH LogLevel is appropriate.	3	2
19009	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure SSH LoginGraceTime is set to one minute or less.	3	2
19009	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure SSH MaxAuthTries is set to 4 or less.	3	2
19009	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure SSH MaxSessions is set to 10 or less.	3	2
19009	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure SSH MaxStartups is configured.	3	2
19009	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure SSH PAM is enabled.	3	2
19009	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure SSH PermitEmptyPasswords is disabled.	3	2
19009	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure SSH PermitUserEnvironment is disabled.	3	2
19009	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure SSH X11 forwarding is disabled.	3	2
19009	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure SSH access is limited.	3	2
19009	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure SSH root login is disabled.	3	2
19009	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure SSH warning banner is configured.	3	2
19009	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure a nftables table exists.	3	2
19009	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure chrony is running as user _chrony.	3	2
19009	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure cryptographic mechanisms are used to protect the integrity of audit tools.	3	2

Rule ID	Description	Level	Count
23505	CVE-2024-52005 affects git	10	1
23505	CVE-2024-52005 affects git-man	10	1
23505	CVE-2025-46835 affects git	10	1
23505	CVE-2025-46835 affects git-man	10	1
23505	CVE-2025-48384 affects git	10	1
23505	CVE-2025-48384 affects git-man	10	1
23505	CVE-2025-54100 affects Microsoft Windows 10 Pro	10	1
23505	CVE-2025-55233 affects Microsoft Windows 10 Pro	10	1
23505	CVE-2025-59505 affects Microsoft Windows 10 Pro	10	1
23505	CVE-2025-59506 affects Microsoft Windows 10 Pro	10	1
23505	CVE-2025-59507 affects Microsoft Windows 10 Pro	10	1
23505	CVE-2025-59508 affects Microsoft Windows 10 Pro	10	1
23505	CVE-2025-59511 affects Microsoft Windows 10 Pro	10	1
23505	CVE-2025-59512 affects Microsoft Windows 10 Pro	10	1
23505	CVE-2025-59514 affects Microsoft Windows 10 Pro	10	1
23505	CVE-2025-59515 affects Microsoft Windows 10 Pro	10	1
23505	CVE-2025-59516 affects Microsoft Windows 10 Pro	10	1
23505	CVE-2025-59517 affects Microsoft Windows 10 Pro	10	1
23505	CVE-2025-60703 affects Microsoft Windows 10 Pro	10	1
23505	CVE-2025-60704 affects Microsoft Windows 10 Pro	10	1