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

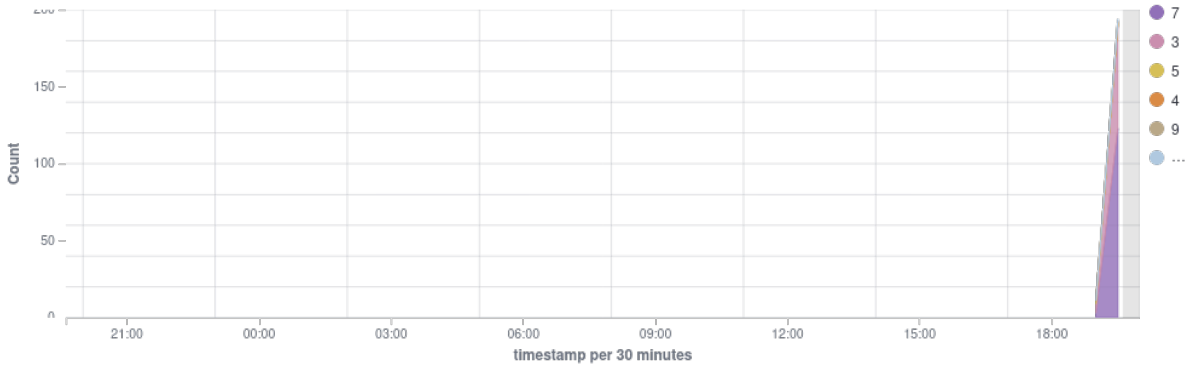
Threat hunting report

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

2024-10-15T19:36:33 to 2024-10-16T19:36:33

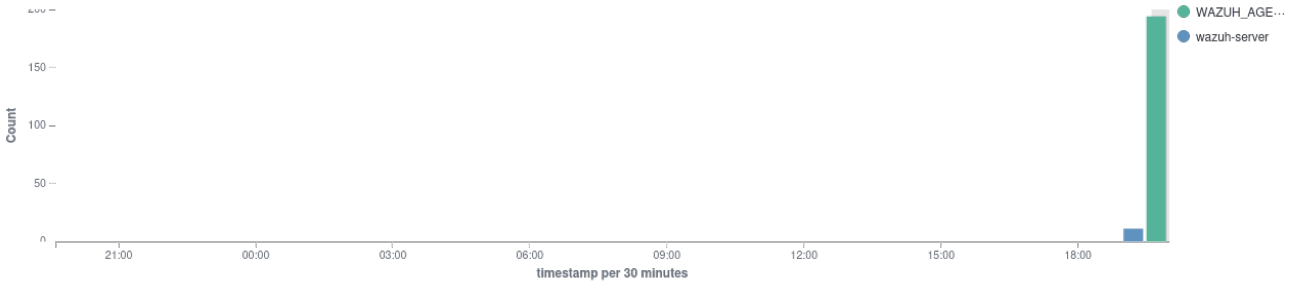
manager.name: wazuh-server

Top 10 Alert level evolution



Top 10 MITRE ATT&CKS

Alerts evolution - Top 5 agents



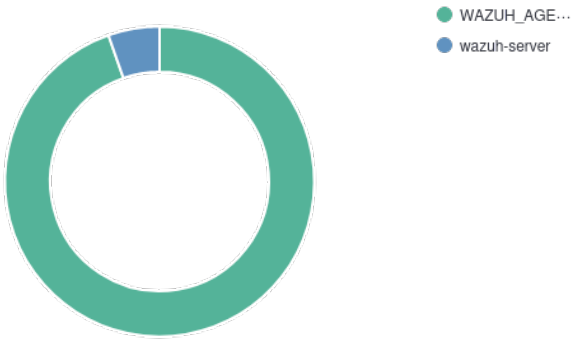
205
- Total -

0
- Level 12 or above alerts -

1
- Authentication failure -

1
- Authentication success -

Top 5 agents



Alerts summary

Rule ID	Description	Level	Count
510	Host-based anomaly detection event (rootcheck).	7	4
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure default deny firewall policy.	7	3
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure NIS Server is not installed.	7	2
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure Uncomplicated Firewall is not installed or disabled.	7	2
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure loopback traffic is configured.	7	2
19009	CIS Amazon Linux 2 Benchmark v2.0.0: Ensure sticky bit is set on all world-writable directories.	3	2
19009	CIS Amazon Linux 2 Benchmark v2.0.0: Ensure updates, patches, and additional security software are installed.	3	2
533	Listened ports status (netstat) changed (new port opened or closed).	7	2
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Disable Automounting.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Disable USB Storage.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure /tmp is configured.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure AIDE is installed.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure AppArmor is enabled in the bootloader configuration.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure Avahi Server is not installed.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure CUPS is not installed.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure DCCP is disabled.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure DHCP Server is not installed.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure DNS Server is not installed.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure FTP Server is not installed.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure GDM is removed or login is configured.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure HTTP Proxy Server is not installed.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure HTTP server is not installed.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure IMAP and POP3 server are not installed.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure IPv6 default deny firewall policy.	7	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure AppArmor is installed.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH HostbasedAuthentication is disabled.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH IgnoreRhosts is enabled.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH LogLevel is appropriate.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH MaxSessions is limited.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH PAM is enabled.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH PermitEmptyPasswords is disabled.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH PermitUserEnvironment is disabled.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure TCP SYN Cookies is enabled.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure Uncomplicated Firewall is installed.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure X Window System is not installed.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure XD/NX support is enabled.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure address space layout randomization	3	1

Rule ID	Description	Level	Count
	(ASLR) is enabled.		
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure all AppArmor Profiles are in enforce or complain mode.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure authentication required for single user mode.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure bogus ICMP responses are ignored.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure broadcast ICMP requests are ignored.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure cron daemon is enabled and running.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure default group for the root account is GID 0.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure journald is configured to compress large log files.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure audit log storage size is configured.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure audit logs are not automatically deleted.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure changes to system administration scope (sudoers) is collected.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure discretionary access control permission modification events are collected.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify date and time information are collected.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify the system's Mandatory Access Controls are collected.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify the system's network environment are collected.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify user/group information are collected.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure file deletion events by users are collected.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure kernel module loading and unloading is collected.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure login and logout events are collected.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure rsyslog default file permissions configured.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure session initiation information is collected.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure successful file system mounts are collected.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system administrator command executions (sudo) are collected.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system is disabled when audit logs are full.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure the audit configuration is immutable.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure unsuccessful unauthorized file access attempts are collected.	3	1
19012	CIS Amazon Linux 2 Benchmark v2.0.0: Ensure sticky bit is set on all world-writable directories.: Status changed from passed to 'not applicable'	5	1
19012	CIS Amazon Linux 2 Benchmark v2.0.0: Ensure updates, patches, and additional security software are installed.: Status changed from passed to 'not applicable'	5	1

Rule ID	Description	Level	Count
19004	SCA summary: CIS Amazon Linux 2 Benchmark v2.0.0: Score less than 50% (41)	7	1
19005	SCA summary: Center for Internet Security Debian Family Linux Benchmark v1.0.0: Score less than 30% (26)	9	1
19010	CIS Amazon Linux 2 Benchmark v2.0.0: Ensure that strong Key Exchange algorithms are used.: Status changed from failed to passed	3	1
501	New wazuh agent connected.	3	1
502	Wazuh server started.	3	1
503	Wazuh agent started.	3	1
506	Wazuh agent stopped.	3	1
5403	First time user executed sudo.	4	1
5404	Three failed attempts to run sudo	10	1
5501	PAM: Login session opened.	3	1
5502	PAM: Login session closed.	3	1
5503	PAM: User login failed.	5	1