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

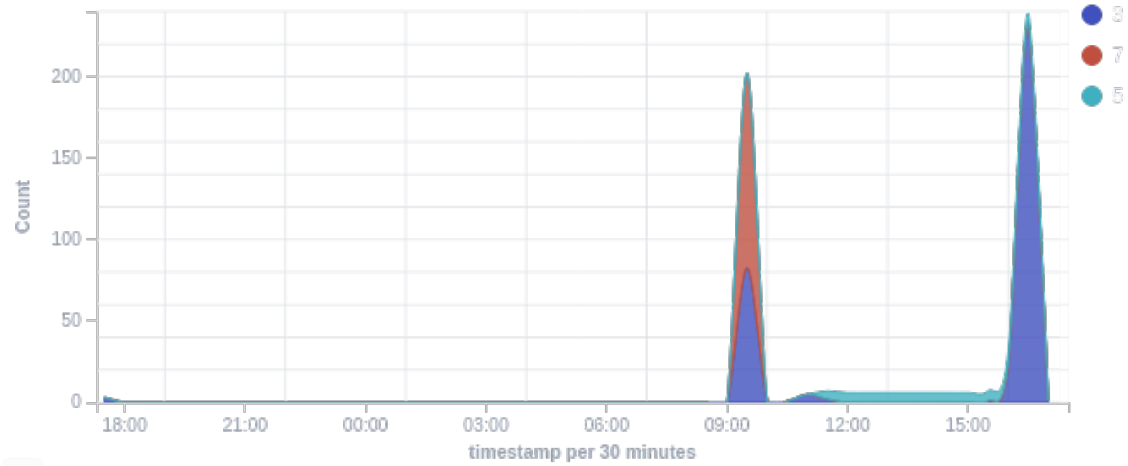
Security events report

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

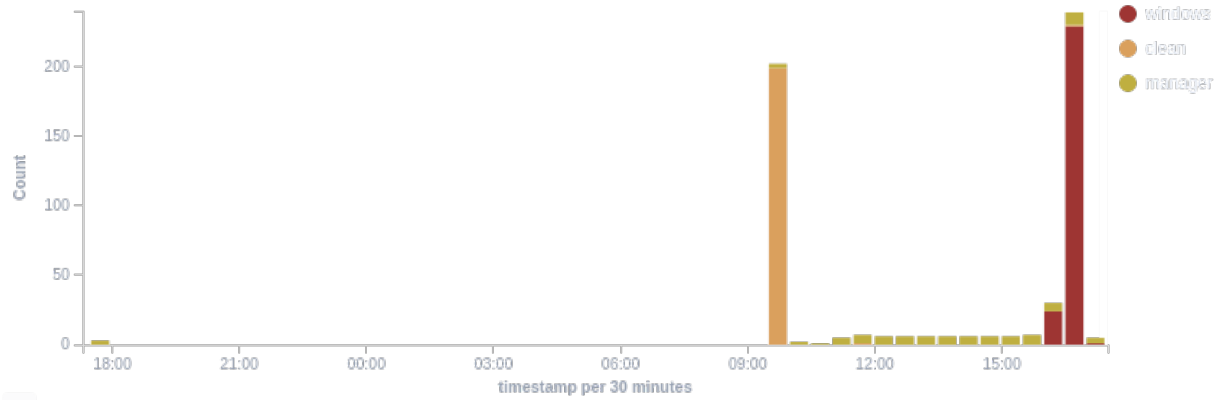
2021-02-16T17:18:05 to 2021-02-17T17:18:05

manager.name: manager

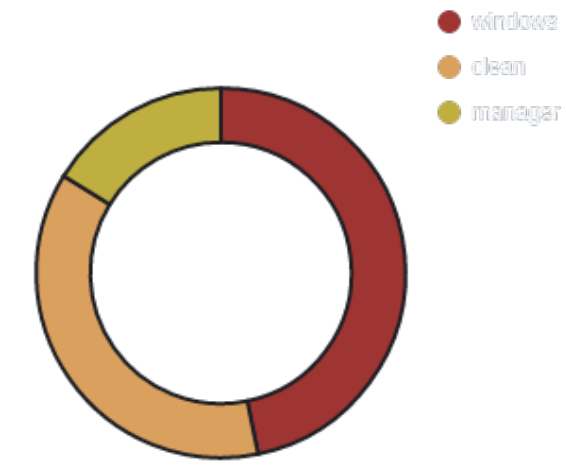
Alert level evolution



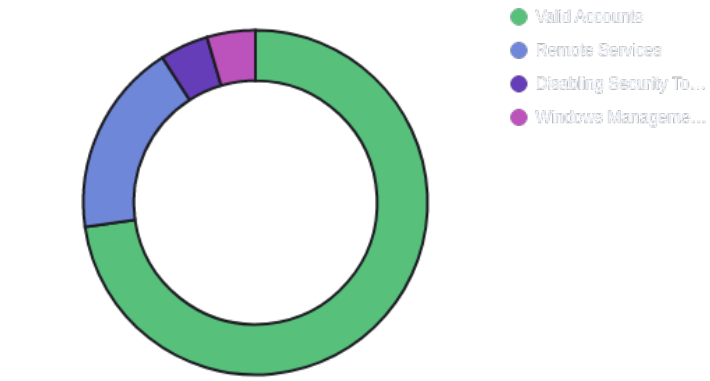
Alerts evolution Top 5 agents



Top 5 agents



Alerts



Alerts summary

Rule ID	Description	Level	Count
61104	Service startup type was changed	3	221
100003	ESquery returned hits for rule 5715	5	69
60106	Windows Logon Success	3	8
60798	The database engine attached a database	3	6
100002	ESquery returned hits for rule 5715	3	5
503	Ossec agent started.	3	5
60797	The database engine detached a database	3	5
5501	PAM: Login session opened.	3	4
5715	sshd: authentication success.	3	4
502	Ossec server started.	3	3
5502	PAM: Login session closed.	3	3
60642	Software Protection service scheduled successfully	3	3
19007	CIS Benchmark for CentOS 7: Ensure SSH Idle Timeout Interval is configured	7	2
19007	CIS Benchmark for CentOS 7: Ensure journald is configured to compress large log files	7	2
19008	CIS Benchmark for CentOS 7: Ensure nfs-utils is not installed or the nfs-server service is masked	3	2
19008	CIS Benchmark for CentOS 7: Ensure permissions on SSH private host key files are configured	3	2
19004	SCA summary: CIS Benchmark for CentOS 7: Score less than 50% (39)	7	2
60643	SLUI.exe launched	3	2
607	Active response: restart-ossec.cmd - add	3	2
19007	CIS Benchmark for CentOS 7: Ensure X11 Server components are not installed	7	1
19007	CIS Benchmark for CentOS 7: Ensure default user shell timeout is configured	7	1
19007	CIS Benchmark for CentOS 7: Disable IPv6	7	1
19007	CIS Benchmark for CentOS 7: Disable USB Storage	7	1
19007	CIS Benchmark for CentOS 7: Ensure /dev/shm is configured	7	1
19007	CIS Benchmark for CentOS 7: Ensure /tmp is configured	7	1
19007	CIS Benchmark for CentOS 7: Ensure AIDE is installed	7	1
19007	CIS Benchmark for CentOS 7: Ensure DCCP is disabled	7	1
19007	CIS Benchmark for CentOS 7: Ensure FirewallD or nftables or iptables-services is installed	7	1
19007	CIS Benchmark for CentOS 7: Ensure ICMP redirects are not accepted	7	1
19007	CIS Benchmark for CentOS 7: Ensure IP forwarding is disabled	7	1
19007	CIS Benchmark for CentOS 7: Ensure IPv6 router advertisements are not accepted	7	1
19007	CIS Benchmark for CentOS 7: Ensure Reverse Path Filtering is enabled	7	1
19007	CIS Benchmark for CentOS 7: Ensure SCTP is disabled	7	1
19007	CIS Benchmark for CentOS 7: Ensure SSH AllowTcpForwarding is disabled	7	1
19007	CIS Benchmark for CentOS 7: Ensure SSH HostbasedAuthentication is disabled	7	1
19007	CIS Benchmark for CentOS 7: Ensure SSH IgnoreRhosts is enabled	7	1
19007	CIS Benchmark for CentOS 7: Ensure SSH LoginGraceTime is set to one minute or less	7	1
19008	CIS Benchmark for CentOS 7: Ensure Avahi Server is not installed	3	1
19008	CIS Benchmark for CentOS 7: Ensure DNS Server is not installed	3	1

Rule ID	Description	Level	Count
19008	CIS Benchmark for CentOS 7: Disable Automounting	3	1
19008	CIS Benchmark for CentOS 7: Ensure CUPS is not installed	3	1
19008	CIS Benchmark for CentOS 7: Ensure DHCP Server is not installed	3	1
19008	CIS Benchmark for CentOS 7: Ensure FTP Server is not installed	3	1
19008	CIS Benchmark for CentOS 7: Ensure HTTP Proxy Server is not installed	3	1
19008	CIS Benchmark for CentOS 7: Ensure HTTP server is not installed	3	1
19008	CIS Benchmark for CentOS 7: Ensure IMAP and POP3 server is not installed	3	1
19008	CIS Benchmark for CentOS 7: Ensure IPv6 default deny firewall policy	3	1
19008	CIS Benchmark for CentOS 7: Ensure IPv6 loopback traffic is configured	3	1
19008	CIS Benchmark for CentOS 7: Ensure IPv6 outbound and established connections are configured	3	1
19008	CIS Benchmark for CentOS 7: Ensure LDAP Server is not installed	3	1
19008	CIS Benchmark for CentOS 7: Ensure LDAP client is not installed	3	1
19008	CIS Benchmark for CentOS 7: Ensure NIS Client is not installed	3	1
19008	CIS Benchmark for CentOS 7: Ensure NIS Server is not installed	3	1
19008	CIS Benchmark for CentOS 7: Ensure SELinux is installed	3	1
19008	CIS Benchmark for CentOS 7: Ensure SELinux is not disabled in bootloader configuration	3	1
19009	CIS Benchmark for CentOS 7: Ensure GDM login banner is configured	3	1
19009	CIS Benchmark for CentOS 7: Ensure nonessential services are removed or masked	3	1
19009	CIS Benchmark for CentOS 7: Ensure ntp is configured	3	1
501	New ossec agent connected.	3	1
504	Ossec agent disconnected.	3	1
60747	WMI Service started successfully	3	1
60776	SessionEnv was unavailable to handle a critical notification event	7	1
60805	The database engine is starting a new instance	3	1
60823	Customer Experience Improvement Program data successfully consolidated	3	1